(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 994 599 A1

(12) EUROPEAN PATENT APPLICATION

published in accordance with Art. 158(3) EPC

(43) Date of publication:
19.04.2000 Bulletin 2000/16

(21) Application number: **99910755.0**

(22) Date of filing: **30.03.1999**

(51) Int. Cl.[7]: **H04L 9/08**, H04L 9/14, H04L 9/32, H04H 1/00

(86) International application number:
PCT/JP99/01606

(87) International publication number:
WO 99/50992 (07.10.1999 Gazette 1999/40)

(84) Designated Contracting States:
DE FR GB

(30) Priority: **01.04.1998 JP 8909898**
09.06.1998 JP 16108298
10.06.1998 JP 16266798

(71) Applicant:
Matsushita Electric Industrial Co., Ltd.
Kadoma-shi, Osaka 571-8501 (JP)

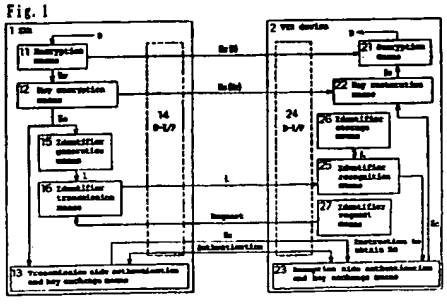
(72) Inventors:
- **NISHIMURA, Takuya**
  Osaka-shi, Osaka 545-0053 (JP)
- **IITSUKA, Hiroyuki**
  Katano-shi, Osaka 576-0033 (JP)
- **YAMADA, Masazumi**
  Moriguchi-shi, Osaka 570-0011 (JP)
- **GOTOH, Shoichi**
  Katano-shi, Osaka 576-0021 (JP)
- **TAKECHI, Hideaki,**
  Lemonflats
  Osaka-shi, Osaka 533-0004 (JP)

(74) Representative:
Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
80538 München (DE)

(54) DATA TRANSMITTING/RECEIVING METHOD, DATA TRANSMITTER, DATA RECEIVER, DATA TRANSMITTING/RECEIVING SYSTEM, AV CONTENT TRANSMITTING METHOD, AV CONTENT RECEIVING METHOD, AV CONTENT TRANSMITTER, AV CONTENT RECEIVER, AND PROGRAM RECORDING MEDIUM

(57) A data transmitting and receiving method for improving transmission and reception efficiency can be obtained by improving the security through update of a control key and reduction of the frequency of the authentication and key exchange process. An STB 1 transmits encrypted digital data Kw (D) obtained by encrypting digital data D using a work key Kw, and an encrypted work key Kc (Kw) obtained by encrypting the Kw using a control key Kc. The Kc is periodically or non-periodically updated, and an identifier L identifying the Kc is assigned to each Kc. A VTR device 2 decrypts the received Kc (Kw) using the Kc obtained by performing the authentication and key exchange process with the STB 1, decrypts the Kw (D) received using the Kw to obtain the D. It is determined whether or not the Kc has been updated while the reception process is suspended by referring to the transmitted L when the reception process is suspended and then resumed. If it is determined that the Kc has been updated, then the authentication and key exchange process is performed again to obtain the updated Kc.

Fig. 1



EP 0 994 599 A1

Description

Technical Field

[0001] The present invention relates to a data transmitting/receiving method, a data transmission apparatus, a data reception apparatus, a data transmission/reception system, and a medium storing a program to direct a computer to perform all or a part of the function of means provided in each of the above described apparatuses.

[0002] In addition, the present invention relates to transmission of AV contents encrypted in different encrypting methods, and reception of the AV contents.

Background Art

[0003] There are two conventional technologies, that is, a first conventional technology, and a second conventional technology, as described below.

[0004] First, the first conventional technology is described below. If data is to be provided only for a specific user, means, etc., then a method for preventing other users or means than the specific user or means from accessing the data is used by the transmission side encrypting and transmitting the data, and the reception side decrypting and uses the encrypted data.

[0005] The above described method is described below by referring to an example in which data is transmitted and received from an STB (Set Top Box, that is, a satellite broadcast receiver) for satellite broadcast to a VTR device for recording satellite broadcast data. In this method, data is encrypted to record correct satellite broadcast data only in the VTR device registered as a subscriber for recording satellite broadcast.

[0006] FIG. 14 shows a configuration of a conventional data transmission and reception system in which an STB for satellite broadcast functions as a data transmission device, and a VTR device functions as a data reception device. The configuration shows only the components relating to the transmission and reception of data between the STB and the VTR device, and reception means, etc. for receiving data from a satellite to the STB, and recording means, etc. for recording data to a recording medium in the VTR device are not shown here. The present system includes: an STB 101 for converting an electric wave received from a satellite into AV data and transmitting the data to a VTR device 102; and the VTR device 102 for recording the AV data transmitted from the STB 101 in the recording medium.

[0007] The STB 101 includes: encryption means 111 for periodically or non-periodically updating a work key Kw, performing a first encryption process using the work key Kw on digital data D obtained by converting an electric wave received from a satellite into AV data so that the digital data D can be converted into encrypted digital data Kw (D), and transmitting the result to the VTR device 102; a key encryption means 112 for generating a control key Kc, performing a second encryption process using the control key Kc on the work key Kw so that the work key Kw can be converted into an encrypted work key Kc (Kw), and transmitting the result to the VTR device 102; a transmission side authentication and key exchange means 113 for performing an authentication and key exchange process with the VTR device 102; and a D-I/F (digital interface) 114 for directly transmitting and receiving data to and from a D-I/F 124 of the VTR device 102.

[0008] The VTR device 102 includes: the D-I/F 124 for directly transmitting and receiving data to and from the D-I/F 114 of the STB 101; a reception side authentication and key exchange means 123 for performing an authentication and key exchange process with the transmission side authentication and key exchange means 113 of the STB 101; key restoration means 122 for decrypting the encrypted work key Kc (Kw) using the control key Kc obtained through the reception side authentication and key exchange means 123, and restoring the work key Kw; and decryption means 121 for decrypting the encrypted digital data Kw (D) using the work key Kw restored by the key restoration means 122, and restoring the digital data D.

[0009] The data transmitted from the STB 101 to the VTR device 102 is the encrypted digital data Kw (D), the encrypted work key Kc (Kw), and the control key Kc. However, since the encrypted digital data Kw (D) and the encrypted work key Kc (Kw) are encrypted data, and the control key Kc is transmitted after the transmission side authentication and key exchange means 113 and the reception side authentication and key exchange means 123 perform an authentication process, the system has high security against the third party who is illegally using data.

[0010] Described below is the second conventional technology. As described above, in recent years there has been developed a technology for transmitting AV contents (AV data) such as movies, etc. using a digital signal, and receiving the AV contents.

[0011] A transmission device for transmitting such AV contents encrypts AV contents before transmission to protect the AV contents. A reception device receives and decrypts the encrypted AV contents, and displays the AV contents on the monitor.

[0012] As described above, the transmission device encrypts the AV contents. However, there are plural types of encrypting methods for encrypting the AV contents. For example, if the reception device is a normal domestic electric appliance such as a television, etc., then a "basic encrypting method" referred to as a baseline cipher such as M6, Blowfish, etc. is used corresponding to the domestic electric appliance. On the other hand, if, for example, the reception device is an appliance having a high-level arithmetic operations capability such as a personal computer, etc., then an "extended encrypting method" such as DES or the like which is more complicated and has a higher encryption

level is used.

[0013] As in the conventional technology, the objects of the present invention exist corresponding to each of the first and second conventional technologies. Therefore, the objects are sequentially described below.

[0014] First, the object corresponding to the first conventional technology is described below. As described above, the control key Kc is transmitted after being authenticated. However, if the same control key Kc is continuously used, it may probably be decrypted by the third party. Therefore, the system can have higher security by periodically or non-periodically updating the control key Kc. However, since it is necessary to perform the authentication and key exchange process each time the control key Kc is updated, it is strongly demanded to minimize the frequency of the authentication and key exchange process for the purpose of reducing the load onto the system and improving the transmission and reception efficiency.

[0015] FIG. 15 shows a relationship between the execution of the control key update process and the authentication and that of key exchange process when the control key is updated by the conventional data transmission and reception system. The horizontal axis indicates the passage of time. The bar in the first row indicates that the STB is transmitting a data signal. The arrow in the second row indicates the range in which the same control key Kc is used. FIG. 15 shows that control key Kc [1] is updated into control key Kc [2]. The bars in the third through fifth rows indicate that the VTR device is in a reception state. The ranges in which the bars are broken indicate that the reception is suspended. The two vertical arrows in the third through fifth rows indicate that the authentication and key exchange process has been performed.

[0016] Since the VTR device in case 1 is not suspended after starting the reception, it performs the authentication and key exchange process after starting the reception, and afterwards performs the authentication and key exchange process only when the control key Kc is updated. Since the VTR device in cases 2 and 3 is suspended after starting the reception, it is required to perform the authentication and key exchange process when resuming the reception. Especially, although the VTR device in case 3 is suspended only for a short time without update of the control key Kc when the reception is resumed, the authentication and key exchange process is to be performed again, thereby increasing the total frequency of the authentication and key exchange process to be performed as compared with the other cases.

[0017] The present invention has been developed to solve the above described problems of the conventional data transmitting and receiving method, and the conventional data transmission and reception system, and aims at providing a data transmitting and receiving method, a data transmission apparatus, a data reception apparatus, a data transmission and reception system for improving the transmission and reception efficiency by improving the security by updating a control key, and reducing the frequency of the authentication and key exchange process, and a program recording medium storing a program executed to direct a computer to perform all or a part of the function of means provided in each of the above described apparatuses.

[0018] The second conventional technology has the following problems. If the transmission device used when the second conventional technology is described is an appliance having a high-level arithmetic operations capability, such as a personal computer or the like, transmitting the AV contents through an IEEE 1394 bus, and the reception device receives the AV contents through the IEEE 1394 bus, and if, as described above, the reception device has a high-level arithmetic operations capability, such as a personal computer or the like, then the reception device can decrypt the AV contents although the transmission device uses the "extended encrypting method" by encrypting and transmitting the AV contents, thereby no problems arise.

[0019] However, for example, a normal domestic electric appliance such as a set top box (satellite broadcast receiver) 59 as well as a personal computer 58, that is, a reception device can also be connected to a transmission device 57 through the IEEE 1394 bus as shown in FIG. 16. In this case, assume that the transmission device 57 encrypts and transmits the AV contents in the "extended encrypting method;" The personal computer 58 receives and decrypts the AV contents, and the set top box 59 tries to receive and decrypts the AV contents during the transmission. However, since the set top box 59 cannot use the "extended encrypting method," it cannot decrypt the AV contents.

Disclosure of the Invention

[0020] As described above, the present invention aims at providing, in view of the problem that an AV contents reception device which cannot use a first encrypting method cannot decrypt the AV contents when the AV contents transmission device is transmitting the AV contents encrypted in the first encrypting method, an AV contents transmitting method for allowing the AV contents reception device which cannot use the first encrypting method to decrypt the AV contents when the AV contents transmission device is transmitting the AV contents encrypted in the first encrypting method.

[0021] The present invention also aims at providing an AV contents transmitting device for allowing the AV contents reception device which cannot use the first encrypting method to decrypt the AV contents when the AV contents encrypted in the first encrypting method is being transmitted.

[0022] The present invention further aims at providing an AV contents transmitting method and an AV contents receiving method capable of allowing an AV

contents reception device, which is receiving and decrypting the AV contents encrypted in the first encrypting method in addition to an AV contents reception device which cannot use the first encrypting method, to continuously decrypt the AV contents when the above described AV contents transmitting method is used.

[0023] Furthermore, the present invention aims at providing an AV contents reception device, provided in addition to an AV contents reception device which cannot use the first encrypting method and which the above described AV contents transmission device tries to allow to decrypt the AV contents, for continuously decrypting the AV contents encrypted in the first encrypting method.

[0024] To solve the above-mentioned problems, the 1st invention of the present invention (corresponding to claim 1) is a data transmitting and receiving method in which:

on a transmission side, encrypted digital data obtained by performing a first encryption process on digital data using a work key, and an encrypted work key obtained by performing a second encryption process on the work key using a control key, are transmitted, and

on a reception side, the encrypted work key is received and decrypted using the control key obtained by performing an authentication and key exchange process with the transmission side, and the encrypted digital data is received and decrypted using the decrypted work key, thereby obtaining the digital data, characterized in that:

on said transmission side, the control key is periodically or non-periodically updated, an identifier identifying the control key is assigned for each control key; and

on said reception side, when a reception process is suspended and then resumed, it is determined whether or not the control key has been updated while the reception process is being suspended by referring to the identifier transmitted from the transmission side, and, when it is determined that the control key has been updated, the authentication and key exchange process is performed again, thereby obtaining the updated control key.

[0025] The 2nd invention of the present invention (corresponding to claim 6) is a data transmission apparatus, characterized by comprising:

encryption means periodically or non-periodically updating/generating a work key, performing a first encryption process on digital data using the work key to convert the digital data into encrypted digital data, and transmitting the encrypted digital data to a data reception apparatus;

a key encryption means periodically or non-periodically updating/generating a control key, performing a second encryption process on the work key using the control key to convert the work key into encrypted work key, and transmitting the encrypted work key to the data reception apparatus;

a transmission side authentication and key exchange means performing an authentication and key exchange process with the data reception apparatus;

identifier generation means generating an identifier identifying the control key; and

identifier transmission means transmitting the identifier to the data reception apparatus.

[0026] The 3rd invention of the present invention (corresponding to claim 8) is a data reception apparatus, characterized by comprising:

a reception side authentication and key exchange means performing an authentication and key exchange process with a data transmission apparatus;

key restoration means restoring a work key by decrypting an encrypted work key converted by performing a second encryption process on the work key using a control key, said restoring process being performed using the control key obtained through said reception side authentication and key exchange means;

decryption means restoring digital data by decrypting encrypted digital data converted by performing a first encryption process on the digital data using the work key, said decrypting process being performed using the work key restored by said key restoration means; and

identifier recognition means determining whether or not the control key has been updated by referring to an identifier identifying the control key transmitted from said data transmission apparatus at least when a reception process is suspended and then resumed, and, when it is determined that the control key has been updated, instructing said reception side authentication and key exchange means to perform again the authentication and key exchange process to obtain the updated control key.

[0027] The 4th invention of the present invention (corresponding to claim 14) is a data transmission and reception system, characterized by comprising:

a data transmission apparatus according to the present invention and a data reception apparatus according to the present invention.

[0028] The 5th invention of the present invention (corresponding to claim 15) is a computer readable program recording medium, characterized by storing a pro-

gram for directing a computer to perform each function of all or a part of each component of the data transmission apparatus and the data reception apparatus according to the present invention.

[0029] The 6th invention of the present invention (corresponding to claim 16) is an AV contents transmitting method, characterized by comprising the step of:

> encrypting and transmitting AV contents in a second encryption method which can be used by an AV contents reception apparatus which cannot use a first encrypting method and issues an authentication request when an AV contents transmission apparatus transmits the AV contents encrypted in the first encrypting method using a transmission line.

[0030] The 7th invention of the present invention (corresponding to claim 17) is the AV contents transmitting method according to the 6th invention of the present invention, characterized in that when the authentication request is issued, and when there is an AV contents reception apparatus which receives and decrypts AV contents encrypted in the first encrypting method in addition to an AV contents reception apparatus which has issued the authentication request, the AV contents reception apparatus which receives and decrypts the AV contents in the first encrypting method is notified that an encrypting method is switched into the second encrypting method.

[0031] The 8th invention of the present invention (corresponding to claim 18) is the AV contents transmitting method according to the 7th invention of the present invention, characterized in that a notification of switching the encrypting method is given in a predetermined command or is added to the AV contents.

[0032] The 9th invention of the present invention (corresponding to claim 19) is the AV contents transmitting method according to the 8th invention of the present invention, characterized in that information about what encrypting method is used as the second encrypting method after the switch is given in a predetermined command or is added to the AV contents.

[0033] The 10th invention of the present invention (corresponding to claim 20) is the AV contents transmitting method according to the 8th invention of the present invention, characterized in that an encryption key or a seed of the encryption key used in the second encrypting method after the switch is given in a predetermined command or is added to the AV contents.

[0034] The 11th invention of the present invention (corresponding to claim 21) is the AV contents transmitting method according to the 6th invention of the present invention, characterized in that a switching timing of the encrypting method is an updating timing for an encryption key in the first encrypting method used before the authentication request is issued.

[0035] The 12th invention of the present invention (corresponding to claim 22) is the AV contents transmitting method according to the 7th invention of the present invention, characterized in that a notification that the encrypting method is to be switched into the second encrypting method, and information about a switching timing of the encrypting method are transmitted to at least the AV contents reception apparatus which receives and decrypts the AV contents encrypted in the first encrypting method.

[0036] The 13th invention of the present invention (corresponding to claim 23) is the AV contents transmitting method according to the 6th invention of the present invention, characterized in that:

> said AV contents transmission apparatus stores an AV contents reception apparatus which issued the authentication request; and
> it is determined whether or not a command requesting an encryption key for decryption of the AV contents or a seed of the encryption key is received from the AV contents reception apparatus, and when the command is not received, the encrypting method is switched from the second encrypting method to the first encrypting method.

[0037] The 14th invention of the present invention (corresponding to claim 24) is the AV contents transmitting method according to the 6th invention of the present invention, characterized in that:

> said AV contents transmission apparatus checks the encrypting method available by each of the AV contents reception apparatus which issued the authentication request and the other AV contents reception apparatus; and
> when an AV contents reception apparatus transmitting a command requesting an encryption key for decryption of the AV contents and the seed of the encryption key is an AV contents reception apparatus capable of using the first encrypting method, the encrypting method is switched from the second encrypting method to the first encrypting method.

[0038] The 15th invention of the present invention (corresponding to claim 25) is a program recording medium, characterized by storing a program for directing a computer to perform each function of all or a part of each step of the AV contents transmitting method according to any one of the 6th through 14th inventions of the present invention.

[0039] The 16th invention of the present invention (corresponding to claim 26) is an AV contents receiving method, characterized by comprising the steps of:

> receiving AV contents transmitted from the AV contents transmitting method according to any one of the 6th through 14th inventions of the present invention; and

decrypting the encrypted AV contents based on an encrypting method used when the AV contents are encrypted and using an encryption key used in the encrypting method or a seed of the encryption key.

[0040] The 17th invention of the present invention (corresponding to claim 27) is the AV contents receiving method according to the 16th invention, characterized in that:

there is information about switching the encrypting method transmitted together with or in the AV contents in the AV contents transmitting method according to any one of the 6th through 14th inventions of the present invention; and
when the information contains none or one of the information about what encrypting method is used after the switch, and the encryption key used in the encrypting method or a seed of the encryption key, the information about what encrypting method is used after the switch, or the encryption key used in the encrypting method or a seed of the encryption key, whichever is not contained in the information relating to the switch of the encrypting method, is to be transmitted to the AV contents transmission apparatus.

[0041] The 18 invention of the present invention (corresponding to claim 28) is a program recording medium, characterized by storing a program for directing a computer to perform each function of all or a part of each step of the AV contents receiving method according to the 16th or 17th invention of the present invention.

[0042] The 19th invention of the present invention (corresponding to claims 29) is an AV contents transmission apparatus, characterized by comprising:

encrypting method selection means selecting an encrypting method used when AV contents to be transmitted are encrypted;
encryption key generation means generating an encryption key for encrypting AV contents corresponding to the encrypting method selected by said encrypting method selection means;
encryption means receiving AV contents, also receiving the encryption key from the encryption key generation means, and encrypting the AV contents; and
a transmission side authentication and key exchange means performing an authentication and key exchange process with an AV contents reception apparatus, wherein
when the AV contents reception apparatus is transmitting the AV contents encrypted in the first encrypting method selected by said encrypting method selection means, and when the AV contents reception apparatus which cannot use the first encrypting method issues an authentication request, the transmission side authentication and key exchange means performs an authentication process with the AV contents reception apparatus which issued the authentication request, and
said encrypting method selection means switches the encrypting method into the second encrypting method the AV contents reception apparatus which issued the authentication request can use.

[0043] The 20th invention of the present invention (corresponding to claim 30) is the AV contents transmission apparatus according to the 19th invention of the present invention, characterized by further comprising an encrypting method notification means issues a notification that the encrypting method is switched into the second encrypting method to an AV contents reception apparatus which is provided in addition to the AV contents reception apparatus which issues an authentication request, and receives and decrypts the AV contents encrypted in the first encrypting method.

[0044] The 21st invention of the present invention (corresponding to claim 31) is the AV contents transmission apparatus according to the 19th invention of the present invention, characterized in that;

said encryption key generation means periodically or non-periodically updates the encryption key;
said encrypting method selection means switches the encrypting method into the second encrypting method at a timing of said encryption key generation means updating the encryption key in the first encrypting method.

[0045] The 22nd invention of the present invention (corresponding to claim 32) is the AV contents transmission apparatus according to the 19th invention of the present invention, characterized in that

said transmission side authentication and key exchange means stores an AV contents reception apparatus which issued the authentication request, and
it is determined whether or not a command requesting an encryption key for decryption of the AV contents or a seed of the encryption key is received from the AV contents reception apparatus; and
when the command is not received, said encryption key generation means switches the encrypting method from the second encrypting method to the first encrypting method.

[0046] The 23rd invention of the present invention (corresponding to claim 33) is the AV contents transmission method according to the 29th invention of the present invention, characterized in that:

said transmission side authentication and key

exchange means checks the encrypting method available by each of the AV contents reception apparatus which issued the authentication request and the other AV contents reception apparatus; and

when an AV contents reception apparatus transmitting a command requesting an encryption key for decryption of the AV contents and the seed of the encryption key is an AV contents reception apparatus capable of using the first encrypting method, said encryption key generation means switches the encrypting method from the second encrypting method to the first encrypting method.

[0047] The 24 invention of the present invention (corresponding to claim 34) is the AV contents reception apparatus according to any one of the 19th through 23rd inventions of the present invention, characterized by further comprising:

a reception side authentication and key exchange means performing an authentication and key exchange process with said AV contents reception apparatus;

encrypting method storage means receiving and information about an encrypting method used in encrypting AV contents from said AV contents transmission apparatus; and

decryption means receiving encrypted AV contents from the AV contents transmission apparatus, receiving an encryption key or a seed of the encryption key from said AV contents transmission apparatus, and decrypting the encrypted AV contents using the encryption key of the seed of the encryption key based on the encrypting method stored in said encrypting method storage means.

[0048] The 25th invention of the present invention (corresponding to claim 35) is the AV contents reception apparatus according to the 24th invention of the present invention, characterized by further comprising:

request means requesting transmitting information such that;

there is information about switching the encrypting method transmitted together with or in the AV contents from the AV contents transmission apparatus according to any one of the 19th through 23rd inventions of the present invention, and

when the information contains none or one of the information about what encrypting method is used after the switch, and the encryption key used in the encrypting method or a seed of the encryption key, the information about what encrypting method is used after the switch, or the encryption key used in the encrypting method or a seed of the encryption key, whichever is not contained in the information is to be transmitted.

Brief Description of the Drawings

[0049]

FIG. 1 shows a configuration of the data transmission and reception system according to a first embodiment of the present invention;

FIG. 2 is a flowchart showing the procedure in the method in which an STB 1 encrypts and transmits data, and a VTR device 2 decrypts the encrypted data and uses the data in the data transmission and reception system according to the first embodiment of the present invention;

FIG. 3 is a flowchart showing the procedure in which a reception process is suspended, and then the reception is resumed in the data transmission and reception system according to the first embodiment of the present invention;

FIG. 4 shows the relationship between the execution of a control key update process and that of an authentication and key exchange process of the data transmission and reception system according to the first embodiment of the present invention;

FIG. 5 shows the configuration of the data transmission and reception system according to a second embodiment of the present invention;

FIG. 6 is a flowchart showing the procedure in the method in which an STB 1 encrypts and transmits data, and a VTR device 2 decrypts the encrypted data and uses the data in the data transmission and reception system according to the second embodiment of the present invention;

FIG. 7 is a flowchart showing the procedure in which a reception process is suspended, and then the reception is resumed in the data transmission and reception system according to the second embodiment of the present invention;

FIG. 8 shows the relationship between the execution of a control, key update process and that of an authentication and key exchange process of the data transmission and reception system according to the second embodiment of the present invention;

FIG. 9 is a block diagram of an AV contents communications system according to a third embodiment of the present invention;

FIG. 10 shows the configuration of the data containing AV contents and a command transmitted by an AV contents transmission device 31 of the AV contents communications system according to the third embodiment of the present invention;

FIG. 11 is a flowchart showing a part of the operations of the AV contents transmission device 31 of the AV contents communications system according to the third embodiment of the present invention;

FIG. 12 is a flowchart showing a part of the operations of an first AV contents reception device 32 of the AV contents communications system according to the third embodiment of the present invention;

FIG. 13 is another flowchart different from Fig. 11 showing a part of the operations of the AV contents transmission device 31 of the AV contents communications system according to the third embodiment of the present invention;

FIG. 14 shows the configuration of the conventional data transmission and reception system;

FIG. 15 shows a relationship between the execution of a control key update process and an authentication and that of key exchange process when a control key is updated in the conventional data transmission and reception system; and

FIG. 16 illustrates the explanation of the problem of the second conventional technology.

(Description of Symbols)

[0050]

1, 101 STB
2, 102 VTR device
11, 111 Encryption means
12, 112 Key encryption means
13, 113 Transmission side authentication and key exchange means
14, 24, 114, 124 D-I/F
15 Identifier generation means
16 Identifier transmission means
21, 121 Decryption means
22, 122 Key restoration means
23, 123 Reception side authentication and key exchange means
25 Identifier recognition means
26 Identifier storage means
27 Identifier request means
31 AV contents transmission device
32 First AV contents reception device
33 Second AV contents reception device
34 Antenna
35, 36 Monitor
37 Reception means
38 Encryption means
39 Kco generation means
40 Encrypting method selection means
41, 46, 53 AKE means
42 Encrypting method change notification means
43 Kco request command response means
44, 45, 52 Data transfer means
47 Encrypting method notification detection means
48, 54 Kco request command issue means
49, 55 Kco storage means
50 Encrypting method storage means
51, 56 Decryption means
57 Transmission device
58 Personal computer
59 Set top box (satellite broadcast receiver)

Best Mode for Carrying Out the Invention

[0051] The embodiments of the present invention will be described below with reference to the attached drawings.

(First Embodiment)

[0052] The first embodiment of the present invention will be described below with reference to the attached drawings.

[0053] FIG. 1 shows the configuration of the data transmission and reception system according to the first embodiment of the present invention. The configuration only shows the components relating to the transmission and reception of data between an STB and a VTR device. The reception means, etc. for receiving data from a satellite in an STB, and recording means, etc. in a recording medium in a VTR device are omitted in the attached drawings. The data transmission and reception system according to the present embodiment transmits and receives data to and from a VTR device for recording satellite broadcast data from an STB for a satellite broadcast, and comprises an STB 1 corresponding to the data transmission apparatus according to the present invention, and a VTR device 2 corresponding to the data reception apparatus according to the present invention.

[0054] The STB 1 comprises: encryption means 11 for periodically or non-periodically updating the work key Kw, performing the first encryption process using the work key Kw on the digital data D obtained by converting an electric wave received from a satellite into AV data so that the digital data D can be converted into the encrypted digital data Kw (D), and transmitting the result to the VTR device 2; a key encryption means 12 for periodically or non-periodically updating the control key Kc, performing the second encryption process using the control key Kc on the work key Kw so that the work key Kw can he converted into the encrypted work key Kc (Kw), and transmitting the result to the VTR device 2; a transmission side authentication and key exchange means 13 for performing an authentication and key exchange process with the VTR device 2; a D-I/F (digital interface) 14 for directly transmitting and receiving data to and from a D-I/F 24 of the VTR device 2; identifier generation means 15 for generating an identifier L for specification of the control key Kc; and identifier transmission means 16 for transmitting the identifier L to the VTR device 2.

[0055] The VTR device 2 comprises: the D-I/F 24 for directly transmitting and receiving data to and from the D-I/F 14 of the STB 1; a reception side authentication and key exchange means 23 for performing an authentication and key exchange process with the transmission side authentication and key exchange means 13 of the STB 1; key restoration means 22 for decrypting the encrypted work key Kc (Kw) using the

control key Kc obtained through the reception side authentication and key exchange means 23; decryption means 21 for decrypting the encrypted digital data Kw (D) using the work key Kw restored by the key restoration means 22, and restoring the digital data D; identifier recognition means 25 for determining whether or not the control key Kc has been updated by referring to an identifier L for specification of the control key Kc transmitted from the STB 1 at least when a receiving operation is resumed after being suspended, and for performing again the authentication and key exchange process on the reception side authentication and key exchange means 23 to obtain an updated control key Kc when it is determined that the control key Kc has been updated; identifier storage means 26 for storing a transmitted identifier L; and identifier request means 27 for requesting the identifier transmission means 16 in the STB 1 to transmit the identifier L when the receiving operation is resumed after being suspended.

[0056] A D-I/F of an IEEE 1394 can be a practical example of the D-I/F 14 and 24. It performs two types of transfer, that is, an isochronous transfer appropriate for a transfer of data such as picture, voice, etc. requiring real-time guarantee; and an asynchronous transfer appropriate for a transfer of authentication and commands, etc. data not requiring the guarantee.

[0057] The procedure of the method in which the STB 1 encrypts and transmits data, and the VTR device 2 decrypts the encrypted data and uses the decrypted data in this system will be described below by referring to FIGS. 2 and 3.

[0058] First, The procedure used in the normal transmission and reception processes is described by referring to FIG. 2. FIG. 2 is a flowchart showing the procedure of the method in which the STB 1 encrypts and transmits data, and the VTR device 2 decrypts the encrypted data and uses the decrypted data in this system according to the first embodiment of the present invention. In FIG. 2, the process performed by the STB 1 is shown on the left, and the process performed by the VTR device 2 is shown on the right. The transmission and reception of data between the STB 1 and the VTR device 2 is all performed through the D-I/F 14 and 24. However, in the description below, the explanation about the process is omitted.

[0059] The key encryption means 12 starts transmitting data and simultaneously generates the control key Kc (step S1), and transmits the key to the transmission side authentication and key exchange means 13 and the identifier generation means 15. The identifier generation means 15 generates an identifier L for specification of the control key Kc, and transmits it to the identifier transmission means 16 (step S2). The transmission side authentication and key exchange means 13 performs the authentication and key exchange process with the reception side authentication and key exchange means 23 to transmit the control key Kc to the VTR device 2 (steps S3 and S4). At this time, the identifier transmission means 16 transmits the identifier L corresponding to the transmitted control key Kc to the identifier recognition means 25. On the VTR device 2 side, the reception side authentication and key exchange means 23 transmits the received control key Kc to the key restoration means 22, and the identifier recognition means 25 transmits the received identifier L to the identifier storage means 26 and stores it therein (step S5). At this time, the identifier storage means 26 overwrites the old identifier L previously stored in the identifier storage means 26.

[0060] On the other hand, on the STB 1 side, the encryption means 11 generates the work key Kw (step S6), and transmits it to the key encryption means 12. The key encryption means 12 performs the second encryption process on the work key Kw using the control key Kc generated in step S1, converts it into the encrypted work key Kc (Kw), and transmits it to the key restoration means 22 (step S7). On the VTR device 2 side, the key restoration means 22 decrypts the encrypted work key Kc (Kw) transmitted from the key encryption means 12 using the control key Kc received by the reception side authentication and key exchange means 23 in step S4, restores the work key Kw, and transmits it to the decryption means 21 (step S8).

[0061] On the STB 1 side, the encryption means 11 performs the first encryption process on the digital data D obtained by converting the electric wave received from a satellite into AV data using the work key Kw generated in step S6, converts it into the encrypted digital data Kw (D), and transmits the result to the decryption means 21 (step S9). On the side of VTR device 2, the decryption means 21 decrypts the received encrypted digital data Kw (D) using the work key Kw restored in step S8, and restores the digital data D (step S10).

[0062] On the VTR device 2 side, if the reception process is suspended for any reason, and the process has to be resumed, then control is passed to A shown in FIG. 3. If the reception process is not suspended, then control is passed to step S12 (step S11). If the reception process does not terminate, then control is passed to step S13 (step S12). Refer to the explanation described later if the reception process is suspended, and the process is to be resumed.

[0063] In step S9, if the data in 1 means has been completed, then it is determined whether or not the work key Kw is to be updated for the next means (step S13). If yes, then control is passed to step S6, and the process similar to that of the above described procedure is performed. If the work key Kw is not updated, then it is determined whether or not the control key Kc is to be updated (step S14). If yes, control is passed to step S1, and the process similar to that of the above described procedure is performed. Provided, there can be the case in which the control key Kc is updated, but the work key Kw is not updated. In this case, the process in step S6 is omitted. When the control key Kc is not updated, control is passed to step S9 (step S15), except

the termination of the transmission, and after this, the process similar to that of the above described procedure is performed.

[0064] Next, the procedure of resuming the reception process after the process is suspended will be described below by referring to FIG. 3. FIG. 3 is a flowchart of the procedure used when the reception process is resumed after being suspended in the data transmission and reception system according to the first embodiment of the present invention. Also in FIG. 3, as in FIG. 2, the process performed by the STB 1 is shown on the left, and the process performed by the VTR device 2 is shown on the right. Furthermore, as in FIG. 2, the data transmission and reception between the STB 1 and the VTR device 2 is performed through the D-I/F 14 and 24, but the explanation is also omitted in the following description.

[0065] In step S11 shown in FIG. 2, if the reception process is suspended, and is to be resumes, then the identifier request means 27 requests the identifier transmission means 16 to transmit an identifier L (step S16). In response to the request, the identifier transmission means 16 transmits the identifier L to the identifier recognition means 25 (step S17). The identifier recognition means 25 compares in step S5 the transmitted identifier L with the identifier L stored in the identifier storage means 26. If the transmitted identifier L is different from the stored identifier L, then step S4 shown in FIG. 2 is processed. If they match each other, step S8 in FIG. 2 is processed(steps S18 and S19). When step S4 is processed, the reception side authentication and key exchange means 23 performs the authentication and key exchange process with the transmission side authentication and key exchange means 13 at the instruction of the identifier recognition means 25, thereby obtaining the control key Kc corresponding to the transmitted identifier L (step S4). Then, the process similar to that of the procedure shown in FIG. 2 is performed. When step S8 is processed, then the procedure relating to obtaining the control key Kc is not used, but the key restoration means 22 decrypts the encrypted work key Kc (Kw) using the control key Kc corresponding to the stored identifier L which had been used before suspending the reception process, thereby restoring the work key Kw (step S8). Then, the process similar to that of the procedure shown in FIG. 2 is performed.

[0066] That is, since the transmission and reception process can be performed on the identifier L without the encryption process, etc., the identifier L is transmitted and received before performing the authentication and key exchange process which requires a heavy load on a system, and then it is determined whether or not the control key Kc has been updated according to the identifier L. Only if it has been updated, the load onto the system can be reduced by performing the authentication and key exchange process.

[0067] FIG. 4 shows the execution of relationship between the control key update process and the authentication and key exchange process of the data transmission and reception system according to the first embodiment of the present invention. The horizontal axis indicates the passage of time. The bar in the first row indicates that the STB is transmitting a data signal. The arrow in the second row indicates the range in which the same control key Kc is used. The present Figure shows that Kc [1] is updated into Kc [2]. The bars in the third through fifth rows indicate that the VTR device in each case is in a reception state. The ranges in which the bars are broken indicate that the reception is suspended. The two vertical arrows in the third through fifth rows indicate that the authentication and key exchange process has been performed. The up-arrow indicates that the identifier request means 27 has requested the identifier transmission means 16 to transmit an identifier L. The down-arrow indicates that the identifier transmission means 16 has transmitted an identifier L.

[0068] Since the VTR device in case 1 is not suspended after starting the reception process, it performs the authentication and key exchange process after it starts the reception process as in the conventional example. Afterwards, it performs the authentication and key exchange process only when the control key Kc is updated. The VTR device in case 2 is suspended after starting the reception process as in the conventional example, and resumes the reception process after updating the control key Kc. Therefore, it should be confirmed by transmitting an identifier L, and perform again the authentication and key exchange process as in the conventional example. Since the VTR device in case 3 is suspended for a short time, the control key Kc is not updated when the reception process is resumed. Therefore, it is confirmed by transmitting an identifier L, and the key restoration process can be continued without performing again the authentication and key exchange process using the control key Kc used before the reception process is suspended. That is, as compared with the conventional technology, the data transmission and reception system according to the present embodiment can reduce the frequency of performing the authentication and key exchange process which requires a heavy load onto the system.

(Second Embodiment)

[0069] The second embodiment of the present invention will be described below with reference to the attached drawings. The point different from the above described first embodiment is that the data reception apparatus according to the present invention does not comprise identifier request means according to the present invention. Therefore, according to the present embodiment, components also used in the above described first embodiment are assigned the same codes, and the detailed explanation is omitted here. In addition, unless specifically described, refer to the descriptions in the first embodiment.

[0070] FIG. 5 shows the configuration of the data transmission and reception system according to the second embodiment of the present invention. The configuration of the data transmission and reception system according to the present embodiment is different from the configuration of the data transmission and reception system according to the first embodiment shown in FIG. 1 in that the VTR device 2 does not comprise the identifier request means 27, that the encryption means 11 of the STB 1 does not update the work key Kw after the control key Kc is updated until the authentication and key exchange process is completed on the control key Kc; and that the identifier transmission means 16 of the STB 1 has the function of periodically or non-periodically transmitting an identifier L to the VTR device 2.

[0071] According to the present embodiment, the identifier transmission means 16 transmits an identifier L to the VTR device 2 each time the work key Kw is updated, and the encrypted work key Kc (Kw) corresponding to the updated work key Kw and simultaneously the identifier L corresponding to the control key Kc at that time are transmitted together. However, the present embodiment is not limited to this application, but the transmission timing can be periodically or non-periodically set only if the updated Kc can be transmitted to the VTR device 2 without fail.

[0072] The procedure of the method of the STB 1 encrypting and transmitting data, and the VTR device 2 decrypting and using the encrypted data in the present system will be described below with reference to FIGS. 6 and 7.

[0073] First, the procedure used in the normal transmission and reception process will be described with FIG. 6. FIG. 6 is a flowchart showing the procedure of the method of the STB 1 encrypting and transmitting data, and the VTR device 2 decrypting and using the encrypted data in the data transmission and reception system according to the second embodiment of the present invention. In the procedure of the normal transmission and reception process, the different point as compared with steps S1 through S15 shown in FIG. 2 described about the first embodiment is that, when the key encryption means 12 transmits the encrypted work key Kc (Kw) to the key restoration means 22 in step S7, the identifier transmission means 16 transmits an identifier L corresponding to the transmitted Kc to identifier recognition means 25, and that, in step S8, the identifier recognition means 25 transmits the received L to the identifier storage means 26 for storage. Other points are the same as in the first embodiment. Therefore, the detailed explanation is omitted here.

[0074] The procedure used when the reception process is suspended and then resumed will be described with reference to FIG. 7. FIG. 7 is a flowchart showing the procedure in which the reception process is suspended and then resumed in the data transmission and reception system according to the second embodiment of the present invention. In FIG. 7, unless specifically described, refer to the descriptions given by referring to FIG. 3.

[0075] In step S11 shown in FIG. 6, when the reception process is suspended and then resumed, an active process is not performed on the VTR device 2 side, but data from the STB 1 is waited for. As in the above described step S7, when the key encryption means 12 transmits the encrypted work key Kc (Kw) to the key restoration means 22, the identifier transmission means 16 transmits an L corresponding to the transmitted Kc to the identifier recognition means 25 (step S66). Therefore, the identifier recognition means 25 compares the transmitted L with the L stored in the identifier storage means 26 in step S5 or S8. If the transmitted L is different from the stored L, then control is passed to step S4 shown in FIG. 6. If they match each other, control is passed to step S8 shown in FIG. 6 (steps S67 and S68). When step S4 is processed, the reception side authentication and key exchange means 23 performs the authentication and key exchange process with the transmission side authentication and key exchange means 13 at an instruction from the identifier recognition means 25 to obtain the control key Kc corresponding to the transmitted L (step S4), and then performs the process in the above described procedure shown in FIG. 6. When step S8 is processed, the procedure for obtaining the Kc is not used, but the key restoration means 22 decrypts the encrypted work key Kc (Kw) using the Kc corresponding to the stored L, which had been used before the reception process was suspended, and then restores the work key Kw (step S8). Then, the processes in the procedure shown in FIG. 6 are performed.

[0076] That is, since an identifier L can be transmitted or received without an encryption process, etc., the identifier L is transmitted or received before performing the authentication and key exchange process which brings a heavy load onto the system, and it is then determined whether or not the control key Kc has been updated according to the identifier L. Only if it has been updated, the authentication and key exchange process is performed to reduce the load onto the system.

[0077] In addition, according to the present embodiment, the encryption means 11 of the STB 1 does not update the work key Kw until the authentication and key exchange process has been completed on the updated control key Kc after the control key Kc was updated, thereby preventing the demerit that the update result of the Kw cannot be obtained during the authentication and key exchange process.

[0078] FIG. 8 shows the relationship between the execution of the control key update process and that of the authentication and key exchange process of the data transmission and reception system according to the second embodiment of the present invention. The horizontal axis indicates the passage of time. The bar in the first row indicates that the STB is transmitting a data signal. The arrow in the second row indicates the range

in which the same control key Kc is used. The present Figure shows that control key Kc [1] is updated into control key Kc [2] in the middle of the process. The bars in the third through fifth rows indicate that the VTR device in each case is in a reception state. The ranges in which the bars are broken indicate that the reception is suspended. The two vertical arrows in the third through fifth rows indicate that the authentication and key exchange process has been performed. The down-arrow indicates that the identifier transmission means 16 has transmitted an identifier L. As described above, since the identifier transmission means 16 has transmitted an L corresponding to the Kc to be transmitted to the identifier recognition means 25 when the key encryption means 12 transmits the encrypted work key Kc (Kw) to the key restoration means 22, the down-arrow indicating this frequently occurs regardless of the reception state of the VTR device.

[0079] Since the VTR device in case 1 is not suspended during the reception process after starting the process, the authentication and key exchange process is performed after starting the reception process as in the conventional example. Afterwards, only the authentication and key exchange process has to be performed when the control key Kc is updated. The VTR device in case 2 is suspended after starting the reception process as in the conventional example, and resumes the reception process after updating the control key Kc. Therefore, it should be confirmed by transmitting an identifier L, and perform again the authentication and key exchange process as in the conventional example. Since the VTR device in case 3 is suspended for a short time, the control key Kc is not updated when the reception process is resumed. Therefore, it is confirmed by transmitting an identifier L, and the key restoration process can be continued without performing again the authentication and key exchange process using the control key Kc used before the reception process is suspended. That is, as compared with the conventional technology, the data transmission and reception system according to the present embodiment can reduce the frequency of performing the authentication and key exchange process which requires a heavy load onto the system in case 3.

[0080] The data transmission apparatus of the data transmission and reception system according to the second embodiment has been described as having the function according to claim 7 of the present invention. However, without the function, the effect of improving the transmission and reception efficiency can be realized by reducing the frequency of performing the authentication and key exchange process. Although the data transmission apparatus in the data transmission and reception system according to the first embodiment has the above described function, the effect obtained by the data transmission and reception system according to the second embodiment can also be obtained.

[0081] In addition, the data transmission and reception system and the data reception apparatus according to the above described first and second embodiments have been described as comprising the identifier storage means according to the present invention. However, they are not limited to this configuration. That is, the identifier recognition means according to the present invention only has to be configured in such a way at least that it can be determined whether or not the control key has been updated by referring to an identifier, which is transmitted from the data transmission apparatus, for specification of the control key when the reception process is resumed after being suspended.

[0082] Furthermore, the data transmitting and receiving method, the data transmission and reception system, the data transmission apparatus, and the data reception apparatus have been described in the first and second embodiments as transmitting and receiving data between the STB of the satellite broadcast and the VTR device for recording corresponding satellite broadcast data. However, they are not limited to this application. That is, data can be encrypted and transmitted from the transmission side, and the encrypted data can be decrypted and used on the reception side, and the key used to encrypting the data can be transmitted by performing the authentication and key exchange process.

[0083] In addition, in the above described first and second embodiments, the data transmission and reception system according to the present invention has been described. The data transmitting and receiving method according to the present invention is also used as described above. In addition, the program recording medium according to the present invention stores a program for directing a computer to perform each of the functions of all or a part of each of the above described methods. For example, it stores a program for directing a computer to perform all or a part of the steps shown in FIGS. 2 and 3, or 6 and 7.

[0084] Furthermore, all or a part of each of the means and components in the data transmission and reception system according to the above described first and second embodiments may be hardware or software having the same function as the hardware.

(Third Embodiment)

[0085] Described below is the configuration of the AV contents communications system according to the third embodiment of the present invention.

[0086] FIG. 9 is a block diagram showing the AV contents communications system according to the third embodiment of the present invention. As shown in FIG. 9, the AV contents communications system according to the third embodiment of the present invention comprises an AV contents transmission device 31, a first AV contents reception device 32, a second AV contents reception device 33, and an IEEE 1394 bus. FIG. 9 also shows an antenna 34, and monitors 35 and 36.

[0087] The AV contents transmission device 31 comprises reception means 37, encryption means 38, Kco generation means 39, encrypting method selection means 40, AKE means 41, encrypting method change notification means 42, Kco request command response means 43, and data transfer means 44 as shown in FIG. 9.

[0088] The reception means 37 receives AV contents through an anntena 34 external to the AV contents transmission device 31.

[0089] The encryption means 38 can use a basic encrypting method and an extended encrypting method, and inputs the AV contents from the reception means 37, also inputs an encryption key Kco from the Kco generation means 39, uses the encrypting method selected by the encrypting method selection means 40, and encrypts the AV contents using the encryption key Kco. In addition, the AV contents encrypted using the encryption key Kco are defined as Kco (AV contents). The basic encrypting method and the extended encrypting method differ in encryption level. That is, the extended encrypting method has a higher encryption level than the basic encrypting method. In other words, they differ in the length of a digital signal configuring the encryption key Kco for use in the encryption process. For example, the basic encrypting method encrypts AV contents using a 40-bit encryption key Kco while the extended encrypting method encrypts AV contents using a 56-bit encryption key Kco.

[0090] The Kco generation means 39 generates an encryption key Kco for use by the encryption means 38 encrypting the AV contents from the reception means 37, and updates the encryption key Kco every 20 seconds.

[0091] The encrypting method selection means 40 selects an encrypting method used when the encryption means 38 encrypts AV contents.

[0092] The AKE means 41 performs the authentication and key exchange process with the first AV contents reception device 32. If the authentication process has been successfully performed with the first AV contents reception device 32, then an exchange key Kex is issued to the first AV contents reception device 32. Similarly, the AKE means 41 performs the authentication and key exchange process with the second AV contents reception device 33.

[0093] When an encrypting method is switched into another encrypting method, the encrypting method change notification means 42 issues a notification of the change.

[0094] The Kco request command response means 43 inputs a command from the first AV contents reception device 32 and/or the second AV contents reception device 33 requesting to transmit the seed of the latest encryption key Kco updated every 20 seconds, and transmits the seed of encryption key Kco in response to the command.

[0095] The data transfer means 44 communicates data between each of the means of the AV contents transmission device 31 and the first AV contents reception device 32 and/or the second AV contents reception device 33.

[0096] The first AV contents reception device 32 comprises data transfer means 45, AKE means 46, encrypting method notification detection means 47, Kco request command issue means 48, Kco storage means 49, encrypting method storage means 50, and decryption means 51 as shown in FIG. 9.

[0097] The data transfer means 45 communicates data between each of the means of the first AV contents reception device 32 and the AV contents transmission device 31.

[0098] The AKE means 46 performs the authentication and key exchange process with the AV contents transmission device 31. If the authentication process has been successfully performed with the AV contents transmission device 31, then an exchange key Kex is received from the AV contents transmission device 31.

[0099] The encrypting method notification detection means 47 detects which encrypting method is used in encrypting the AV contents from the AV contents transmission device 31.

[0100] The Kco request command issue means 48 issues a command requesting the AV contents transmission device 31 to transmit the seed of encryption key Kco corresponding to an encrypting method detected by the encrypting method notification detection means 47. In addition, the Kco request command issue means 48 receives the seed of encryption key Kco from the AV contents transmission device 31.

[0101] The Kco storage means 49 has a predetermined function required when encrypted AV contents from the AV contents transmission device 31 are decrypted, inputs the exchange key Kex from the AKE means 46, also inputs the seed of the encryption key Kco from the Kco request command issue means 48, and substitutes the exchange key Kex and the encryption key Kco for a predetermined function to generate and store an encryption key Kco. Besides, description regarding the function will be made later.

[0102] The encrypting method storage means 50 stores the encrypting method detected by the encrypting method notification detection means 47.

[0103] The decryption means 51 inputs the encrypted AV contents from the AV contents transmission device 31, also inputs the encryption key Kco from the Kco storage means 49 and the encrypting method from the encrypting method storage means 50, and decrypts the encrypted AV contents using the encryption key Kco according to the encrypting method. The decryption means 51 can use either the basic encrypting method or the extended encrypting method.

[0104] Next, the second AV contents reception device 33 comprises data transfer means 52, AKE means 53, Kco request command issue means 54, Kco storage means 55, and decryption means 56 as shown

in FIG. 9.

[0105] The data transfer means 52 communicates data between each of the means of the second AV contents reception device 33 and the AV contents transmission device 31.

[0106] The AKE means 53 performs the authentication and key exchange process with the AV contents transmission device 31. If the authentication process has been successfully performed between the AKE means 53 and the AV contents transmission device 31, then the AKE means 53 inputs an exchange key Kex from the AV contents transmission device 31.

[0107] The Kco request command issue means 54 issues a command to the AV contents transmission device 31 to transmit the seed of the encryption key Kco corresponding to the basic encrypting method. In addition, the Kco request command issue means 54 inputs the seed of the latest encryption key Kco from the AV contents transmission device 31 in response to the request command.

[0108] The Kco storage means 55 has a predetermined function required in decrypting the encrypted AV contents from the AV contents transmission device 31, inputs the seed of encryption key Kco from the Kco request command issue means 54, also receives the exchange key Kex from the AKE means 53, and substitutes the exchange key Kex and the encryption key Kco for a preliminarily set function to generate and store the encryption key Kco.

[0109] The decryption means 56 inputs the encrypted AV contents from the AV contents transmission device 31, also inputs the encryption key Kco from the Kco storage means 55, and decrypts the encrypted AV contents using the encryption key Kco on the basis of the basic encrypting method. It is assumed that the decryption means 56 can use only the basic encrypting method. That is, the decryption means 56 cannot use the extended encrypting method.

[0110] Next, the IEEE 1394 bus is a transmission line of data communicated among the AV contents transmission device 31, the first AV contents reception device 32, and the second AV contents reception device 33.

[0111] An antenna 34 is provided outside the AV contents transmission device 31, and receives the AV contents. The monitor 35 displays the AV contents from the first AV contents reception device. 32. Similarly, the monitor 36 displays the AV contents from the second AV contents reception device 33.

[0112] Described below are the operations of the AV contents communications system according to the third embodiment of the present invention.

[0113] Before describing in detail the operations of the AV contents communications system shown in FIG. 9, the following situation is assumed for convenience, and the operations of the AV contents communications system are described under the situation.

[0114] First, assume that the AV contents transmission device 31 encrypts the AV contents from the antenna 34 in the extended encrypting method, outputs the result through the IEEE 1394 bus, and the first AV contents reception device 32 receives and decrypts the AV contents during the output process of the AV contents, and then the second AV contents reception device 33 which cannot use the extended encrypting method receives the AV contents and tries to decrypt them.

[0115] Described first are the operations of the AV contents transmission device 31 which encrypts the AV contents from the antenna 34 in the extended encrypting method, and then outputs the result through the IEEE 1394 bus. The AV contents transmission device 31 can use either the extended encrypting method or the basic encrypting method as described above. However, unless specifically requested to output the AV contents encrypted in the basic encrypting method, the extended encrypting method having a stronger encryption effect is used in encrypting the AV contents with the view to more strongly protect the output AV contents.

[0116] First, the encrypting method selection means 40 selects the extended encrypting method, the reception means 37 receives the AV contents through the antenna 34 external to the AV contents transmission device 31, and the encryption means 38 inputs the AV contents from the reception means 37, also receives an encryption key Kco1 from the Kco generation means 39, and then encrypts the AV contents using the encryption key Kco1 in the extended encrypting method. To indicate that the encryption key from the Kco generation means 39 as an encryption key corresponding to the extended encrypting method, it is described as "Kco1". In the following descriptions, the encryption key corresponding to the basic encrypting method other than the extended encrypting method is described as "Kco2". The encryption process is not performed on, for example, a part of the headers of the AV contents. That is, it is assumed that the encryption process is performed such that, when the AV contents are received, the header information about the AV contents may be decrypted without the encryption key Kco1, but the AV contents cannot be decrypted without the encryption key Kco1. In addition, the encryption key Kco1 from the Kco generation means 39 to be used by the encryption means 38 is updated every 20 seconds as described above. Then, the Kco generation means 39 outputs "odd" or "even" as the information as to the timing of the update using the encryption key Kco1. When the "odd" and "even" is switched from each other, each indicates that the encryption key Kco1 used in encrypting the AV contents is switched every 20 seconds before and after the switch between "odd" and "even". Then, the data transfer means 44 inputs the AV contents encrypted using the encryption key Kco1 from the encryption means 38, that is, the Kco (AV contents), also receives "odd" or "even" from the Kco generation means 39, adds "odd" or "even" to the header of the Kco (AV con-

tents) as shown in FIG. 10 (a), and outputs the result to the IEEE 1394 bus. FIG. 10(a) shows the configuration of the AV contents transmitted from the AV contents transmission device 31. FIG. 10(b) is described later.

[0117] Next, as described above, the operations of the AV contents transmission device 31 and the first AV contents reception device 32 up to the point when the first AV contents reception device 32 decrypts the AV contents during the output process of the AV contents encrypted and output through the IEEE 1394 bus by the AV contents transmission device 31.

[0118] At this time, the AKE means 46 of the first AV contents reception device 32 issues, an authentication request to the AKE means 41 of the AV contents transmission device 31, and the AKE means 46 and the AKE means 41 authenticate each other's device. If the authentication process can be successfully performed, then the AKE means 41 outputs an exchange key Kex to the AKE means 46. The exchange key Kex is required in decrypting the encrypted AV contents. Simultaneously, the AKE means 41 determines that the first AV contents reception device 32 can use the extended encrypting method, and does not change the encrypting method. If the AKE means 46 and the AKE means 41 fail in the authentication process, the AKE means 41 does not output the exchange key Kex to the AKE means 46. In this example, it is assumed for convenience of the following description that the AKE means 46 and the AKE means 41 can successfully perform the authentication process.

[0119] Then, the AKE means 46 of the first AV contents reception device 32 receives the exchange key Kex from the AKE means 41 through the data transfer means 45, and outputs it to the Kco storage means 49. The encrypting method notification detection means 47 detects that the AV contents from the AV contents transmission device 31 have been encrypted in the extended encrypting method, and outputs the information, that is, the extended encrypting method, to the encrypting method storage means 50 for storage. Furthermore, the Kco request command issue means 48 issues to the Kco request command response means 43 of the AV contents transmission device 31 a command to transmit the seed of the latest encryption key Kco1 corresponding to the extended encrypting method. Then, it receives the seed of the latest encryption key Kco1 from the Kco request command response means 43 in response to the command, and outputs the seed to the Kco storage means 49. As described above, since the encryption key Kco1 from the AV contents transmission device 31 is updated every 20 seconds, the Kco request command issue means 48 is assumed to issue a command to the Kco request command response means 43 every 20 seconds. Then, the Kco storage means 49 substitutes the exchange key Kex from the AKE means 46 and the seed of encryption key Kco1 from the Kco request command issue means 48 for the predetermined functions as described later (equation 1), and generates and stores the encryption key Kco1. In addition, the seed of the encryption key Kco1 is substituted for the seed in Equation 1.

$$Kco = f(seed, Kex) \qquad \text{[Equation 1]}$$

[0120] Then, the "odd" or "even" in the header of the Kco (AV contents) from the AV contents transmission device 31 is detected, the switch between the "odd" and "even" is determined, and then it is determined which encryption key Kco1 has been used to encrypt the Kco (AV contents) from the AV contents transmission device 31. As described above, the switch between "odd" and "even" indicates the switch of the encryption key Kco1 used in encrypting the AV contents. Furthermore, when the Kco request command response means 43 of the AV contents transmission device 31 receives a command to request to send the seed of the encryption key Kco1 from the Kco request command issue means 48, it outputs the seed of the encryption key Kco1 to the data transfer means 44. Then, the data transfer means 44 outputs a command containing the seed of encryption key Kco1 used in the Kco (AV contents) to the IEEE 1394 bus by using an asynchronous signal other than the Kco (AV contents) as shown in FIG. 10(b). FIG. 10(b) shows the configuration of the command transmitted from the AV contents transmission device 31.

[0121] Finally, the decryption means 51 inputs the encrypted AV contents from the AV contents transmission device 31 through the data transfer means 45, also inputs the encryption key Kco1 from the Kco storage means 49 and the extended encrypting method from the encrypting method storage means 50, decrypts the encrypted AV contents using the encryption key Kco1 based on the extended encrypting method, and outputs the result to the monitor 35. Then, the monitor 35 displays the AV contents from the decryption means 51.

[0122] Described next are the operations of the AV contents transmission device 31, the first AV contents reception device 32, and the second AV contents reception device 33 performed when the second AV contents reception device 33 incapable of using the extended encrypting method decrypts the AV contents when, as described above, the AV contents transmission device 31 encrypts and outputs the AV contents in the extended encrypting method, and the first AV contents reception device 32 decrypts the AV contents. At this time, the operations of the AV contents transmission device 31 are described also with reference to the flowchart shown in FIG. 11.

[0123] The AKE means 53 of the second AV contents reception device 33 issues an authentication request to the AKE means 41 of the AV contents transmission device 31, and the AKE means 53 and the AKE means 41 authenticate each other's devices (step 1 shown in FIG. 11). At this time, the AKE means 53 requests to change the encrypting method for the AV

contents output by the AV contents transmission device 31 into the basic encrypting method, because the second AV contents reception device 33 cannot use the extended encrypting method, but can use only the basic encrypting method. The mutual authentication process can be successfully performed, then the AKE means 41 accepts the request (step 2 shown in FIG. 11), and outputs the information for control of the encrypting method selection means 40 and the encrypting method change notification means 42 to set the basic encrypting method as an encrypting method (step 3 shown in FIG. 11). Then, the AKE means 41 outputs the exchange key Kex to the AKE means 53, and the authentication and key exchange process between the AKE means 41 and the AKE means 53 can be completed (step 4 shown in 11). The exchange key Kex is a key required when the encrypted AV contents are decrypted. When the authentication process performed by the AKE means 53 and the AKE means 41 cannot be successfully performed, the AKE means 41 does not output the exchange key Kex to the AKE means 53, nor does it accept the request to set the basic encrypting method as an encrypting method. However, it is assumed for convenience of the following description that the authentication process between the AKE means 53 and the AKE means 41 can be successfully performed.

[0124] In the AV contents transmission device 31, the encrypting method selection means 40 selects the basic encrypting method according to the information for changing the encrypting method from the AKE means 41, that is, the information for setting the basic encrypting method as an encrypting method, and the information is output to the encryption means 38 and the Kco generation means 39. The encrypting method selection means 40 selects the basic encrypting method by the completion of the authentication and key exchange process between the AKE means 41 and the AKE means 53, that is, by the input of the exchange key Kex at the AKE means 53. Then, after the information for changing the encrypting method into the basic encrypting method has been input, and from the next update timing of the encryption key Kco1 generated in the extended encrypting method, the Kco generation means 39 generates the encryption key Kco2 in the basic encrypting method, and updates it every 20 seconds. Furthermore, the encrypting method change notification means 42 outputs the command to inform that the encrypting method of the AV contents is changed from the extended encrypting method to the basic encrypting method to the encrypting method notification detection means 47 of the first AV contents reception device 32, and outputs a command of the information about the switching timing of the encrypting method to the encrypting method notification detection means 47.

[0125] Afterwards, the encryption means 38 of the AV contents transmission device 31 inputs the AV contents from the reception means 37, also inputs the encryption key Kco2 from the Kco generation means 39, and encrypts the AV contents using the encryption key Kco2 in the basic encrypting method. Furthermore, the Kco generation means 39 outputs "odd" or "even" as the information about what timing the encryption key Kco2 is switched. Then, the data transfer means 44 inputs the AV contents encrypted using the encryption key Kco2 from the encryption means 38, that is, Kco (AV contents), also receives "odd" or "even" from the Kco generation means 39, and adds "odd" or "even" to the header of Kco (AV contents) and outputs the result through the IEEE 1394 bus.

[0126] When the encrypting method for the AV contents from the AV contents transmission device 31 is switched into the basic encrypting method, the second AV contents reception device 33 is allowed to decrypt the AV contents. Then, the operations of the second AV contents reception device 33 decrypting the AV contents are described below.

[0127] First, the AKE means 53 inputs the exchange key Kex from the AKE means 41 of the AV contents transmission device 31 through the data transfer means 52, and outputs it to the Kco storage means 55, The Kco request command issue means 54 issues a command to the Kco request command response means 43 of the AV contents transmission device 31 to transmit the seed of the encryption key Kco2 corresponding to the basic encrypting method, inputs in response to the command the seed of the encryption key Kco2 from the Kco request command response means 43, and outputs the seed to the Kco storage means 55. Then, the Kco storage means 55 substitutes the exchange key Kex from the AKE means 53 and the seed of the encryption key Kco2 from the Kco request command issue means 54 for a predetermined function as described above by the equation 1, and generates and stores the encryption key Kco2. Then, it detects "odd" or "even" from the header of the Kco (AV contents) from the AV contents transmission device 31, determines the switch between "odd" and "even", and specifies which encryption key Kco2 is used to encrypt the Kco ((AV contents) from the AV contents transmission device 31.

[0128] Finally, the decryption means 56 receives the encrypted AV contents from the AV contents transmission device 31 through the data transfer means 52, also inputs The encryption key Kco2 from the Kco storage means 55, decrypts the encrypted AV contents using the encryption key Kco2 in the basic encrypting method, and output the result to the monitor 36. The monitor 36 displays the AV contents from the decryption means 56.

[0129] Thus, when the AV contents transmission device 31 changes the encrypting method for the AV contents into the basic encrypting method, and encrypts and outputs the AV contents, the second AV contents reception device 33 is allowed to decrypt the AV contents, but the first AV contents reception device 32 which receives and decrypts the AV contents encrypted

in the extended encrypting method till then cannot decrypt the AV contents as it is. Described below are the operations of the first AV contents reception device 32 when the AV contents transmission device 31 changes the encrypting method for the AV contents into the basic encrypting method, and when the first AV contents reception device 32 decrypts the AV contents. The operations of the first AV contents reception device 32 are also described by referring to the flowchart shown in 12.

[0130] At this time, as described above, the encrypting method notification detection means 47 of the first AV contents reception device 32 inputs from the encrypting method change notification means 42 of the AV contents transmission device 31 a command informing that the encrypting method for the AV contents is changed from the extended encrypting method to the basic encrypting method, and also inputs a command about the timing of switching the encrypting method (step 1 shown in FIG. 12). The encrypting method notification detection means 47 outputs these two pieces of information to the Kco request command issue means 48 and the encrypting method storage means 50. Then, the Kco request command issue means 48 issues to the Kco request command response means 43 of the AV contents transmission device 31 a command to transmit the seed of the encryption key Kco2 corresponding to the basic encrypting method (step 2 shown in FIG. 12), inputs in return for the command the seed of the encryption key Kco2 from the Kco request command response means 43, and outputs the seed to the Kco storage means 49. Then, the Kco storage means 49 substitutes the exchange key Kex from the AKE means 46 and the seed of the encryption key Kco2 from the Kco request command issue means 48 for a predetermined function, and generates and stores the encryption key Kco2 (step 3 shown in FIG. 12).

[0131] Finally, the decryption means 51 receives the encrypted AV contents from the AV contents transmission device 31 through the data transfer means 45, also receives the encryption key Kco2 from the Kco storage means 49 and the basic encrypting method from the encrypting method storage means 50. Since the decryption means 51 can use the basic encrypting method, it decrypts the encrypted AV contents using the encryption key Kco2 in the basic encrypting method, and outputs the result to the monitor 35 (step 4 shown in FIG. 12). Then, the monitor 35 displays the AV contents from the decryption means 51.

[0132] Thus, although the AV contents transmission device 31 has changed the encrypting method for the AV contents into the basic encrypting method, the first AV contents reception device 32 can decrypt the encrypted AV contents in the basic encrypting method by receiving the information that the encrypting method has been switched into the basic encrypting method, and the information about the switching timing.

[0133] It is possible that the second AV contents reception device 33 stops decrypting the AV contents when the AV contents transmission device 31 changes the encrypting method for the AV contents into the basic encrypting method and transmits the AV contents. Described below are the operations of the AV contents transmission device 31 and the first AV contents reception device 32 performed when the second AV contents reception device 33 stops decrypting the AV contents.

[0134] When the second AV contents reception device 33 stops decrypting the AV contents, the Kco request command issue means 54 of the second AV contents reception device 33 stops issuing to the Kco request command response means 43 of the AV contents transmission device 31 a command to transmit the seed of the encryption key Kco2. That is, the Kco request command response means 43 stops receiving a command from the Kco request command issue means 54. When the Kco request command response means 43 stops receiving a command from the Kco request command issue means 54, it is determined that the second AV contents reception device 33 has stopped decrypting the AV contents. Then, the Kco request command response means 43 notifies the encrypting method change notification means 42 that the second AV contents reception device 33 has stopped decrypting the AV contents.

[0135] Then, the encrypting method change notification means 42 inputs the information from the Kco request command response means 43 that the second AV contents reception device 33 has stopped decrypting the AV contents, and according to the information instructs the encrypting method selection means 40 to switch the encrypting method to be selected from the basic encrypting method to the extended encrypting method, and then outputs to the encrypting method notification detection means 47 of the first AV contents reception device 32, the information that the encrypting method is to be switched from the basic encrypting method to the extended encrypting method together with the information about the switching timing. The encrypting method is switched into the extended encrypting method because, as described above, the extended encrypting method has a higher encryption level than the basic encrypting method, and more strongly protects the AV contents from being decrypted by an illegal device than the basic encrypting method. When the encrypting method is switched from the basic encrypting method to the extended encrypting method, the AKE means 41 is preliminarily designed to store the information that the second AV contents reception device 33 can use only the basic encrypting method, and then, the encrypting method change notification means 42 is designed to determine that the encrypting method is to be switched from the basic encrypting method to the extended encrypting method when the second AV contents reception device 33 stops decrypting the AV contents.

[0136] Then, the encrypting method selection

means 40 switches again the selection of the encrypting method from the basic encrypting method to the extended encrypting method. Thus, after the encrypting method has been switched into the extended encrypting method, each of the means in the AV contents transmission device 31 performs the same operations as those performed when AV contents are encrypted and output based on the extended encrypting method before switching into the basic encrypting method as described above.

[0137] On the other hand, in the first AV contents reception device 32, the encrypting method notification detection means 47 inputs from the encrypting method change notification means 42 of the AV contents transmission device 31 the information that the encrypting method is to be switched from the basic encrypting method to the extended encrypting method together with the information about the switching timing. According to the information, each of the means switches their operations in the decryption process. The switching timing is the same as that when the encrypting method is switched from the extended encrypting method to the basic encrypting method. After the switching process, each of the means of the first AV contents reception device 32 operates as in the process similar to that of decrypting the encrypted AV contents in the extended encrypting method before switching into the basic encrypting method as described above.

[0138] Thus, when the AV contents transmission device 31 is encrypting the AV contents in the basic encrypting method and transmitting the result, and when the second AV contents reception device 33 stops decrypting the AV contents, the AV contents transmission device 31 makes a change such that the AV contents encrypted in the extended encrypting method having a higher encryption level can be transmitted. However, the first AV contents reception device 32 can decrypt the AV contents although the encrypting method has been thus changed from the basic encrypting method to the extended encrypting method.

[0139] The above described third embodiment, the encrypting method change notification means 42 of the AV contents transmission device 31 outputs to the encrypting method notification detection means 47 of the first AV contents reception device 32 a command of the information that the encrypting method of the AV contents is to be changed from the extended encrypting method to the basic encrypting method. However, the encrypting method change notification means 42 may be designed to output to the encrypting method notification detection means 47 the information that the encrypting method for the AV contents is changed from the extended encrypting method to another encrypting method. However, in this case, the encrypting method notification detection means 47 has to request the AV contents transmission device 31 to notify what encrypting method is to be used after a change. Similarly, although the encrypting method change notification means 42 outputs to the encrypting method notification detection means 47 a command of the information about the switching timing from the extended encrypting method to the basic encrypting method, the encrypting method change notification means 42 may also be designed not to output the information about the switching timing of the encrypting method to the encrypting method notification detection means 47. However, in this case, the encrypting method notification detection means 47 has to requests the AV contents transmission device 31 to issue a notification about the switching timing of the encrypting method. In addition, the encrypting method switching information and the switching timing information outputted by the encrypting method change notification means 42 may be provided not only as a command, but also as information added to the AV contents.

[0140] According to the above described third embodiment, the AV contents transmission device 31 outputs the information into what encrypting method the current encrypting method is switched, and then, when the first AV contents reception device 32 requests the AV contents transmission device 31 to transmit the seed of the encryption key Kco corresponding to the encrypting method after the switch, transmits the seed of the encryption key Kco in response to the request. However, when the encrypting method is switched, the AV contents transmission device 31 may output the seed of the encryption key Kco corresponding to the encrypting method after the switch together with the information about the encrypting method after the switch. In addition, although the AV contents transmission device 31 outputs the seed of the encryption key Kco, it also may output the encryption key Kco itself, or the encryption key Kco encrypted using the exchange key Kex. In this case, on the reception side, not a seed, but the encryption key Kco itself, or the encryption key Kco encrypted using the exchange key Kex is used. In addition, the seed of the encryption key Kco is transmitted through a command, but the encryption key Kco and the seed thereof may be transmitted either in a command or as the information added to the AV contents for transmission.

[0141] In addition, according to the third embodiment described above, the Kco generation means 39 of the AV contents transmission device 31 updates the encryption key Kco every 20 seconds, but the interval of the Kco generation means 39 updating the encryption key Kco is not limited to every 20 seconds. The encryption key Kco may be updated either periodically or non-periodically.

[0142] According to the third embodiment described above, the AV contents transmission device 31 stores the second AV contents reception device 33, from where determines whether or not a command for requesting the seed of the encryption key Kco2 for decryption of the AV contents has been received. If the command stops, the encrypting method is switched

from the extended encrypting method to the basic encrypting method. However, the AV contents transmission device 31 can check what encrypting method can be used in each of the first AV contents reception device 32 and the second AV contents reception device 33. If all the AV contents reception devices transmitting a command to request the seed of the encryption key Kco for decryption of the AV contents can use the extended encrypting method, then the encrypting method can be switched from the basic encrypting method to the extended encrypting method.

[0143] In addition, according to the third embodiment described above, when the AV contents transmission device 31 switches the encrypting method from the extended encrypting method to the basic encrypting method, the AV contents transmission device 31 first performs the authentication process with the second AV contents reception device 33. If the process is successfully performed, the encrypting method is switched from the extended encrypting method to the basic encrypting method. However, as shown in 13, after the AV contents transmission device 31 has received the authentication request from the second AV contents reception device 33 (step 1 shown in FIG. 13), the encrypting method is switched from the extended encrypting method to the basic encrypting method (step 2 shown in FIG. 13) regardless of the success of the mutual authentication. If the authentication process can be successfully performed after the switch (step 3 shown in FIG. 13), then the basic encrypting method can be specified (step 5 shown in FIG. 13). If the authentication process in step 3 shown FIG. 13 fails, the encrypting method can be switched from the basic encrypting method to the extended encrypting method (step 4 shown in FIG. 13)

[0144] In addition, according to the third embodiment described above, the AV contents transmission device 31 performs the authentication process with the second AV contents reception device 33. If the authentication process is successfully performed, the encrypting method is switched from the extended encrypting method to the basic encrypting method. However, when the AV contents transmission device 31 receives an authentication request from the second AV contents reception device 33, it switches the encrypting method from the extended encrypting method to the basic encrypting method regardless of the success of the authentication process, and the AV contents may be encrypted in the switched-to basic encrypting method. However, in this case, if the authentication process fails between the AV contents transmission device 31 and the second AV contents reception device 33, then the AV contents transmission device 31 does not output the exchange key Kex to the second AV contents reception device 33. Therefore, the AV contents from the AV contents transmission device 31 can be protected from being decrypted by an illegal device. On the other hand, when the AV contents transmission device 31 receives an authentication request from the second AV contents reception device 33, and outputs the encrypted AV contents after switching the encrypting method to the basic encrypting method, the first AV contents reception device 32 receives from the AV contents transmission device 31 the information that the encrypting method is switched into the basic encrypting method as described above in the third embodiment, also receives the AV contents encrypted in the basic encrypting method from the AV contents transmission device 31, and the AV contents are decrypted in the basic encrypting method. On the other hand, the AV contents transmission device 31 changes again into the extended encrypting method when the AV contents transmission device 31 determines that the second AV contents reception device 33 is illegal.

[0145] In addition, all or a part of the components means and elements of the AV contents communications system according to the aforementioned third embodiment may be either hardware, or software having the same function as the hardware.

[0146] Furthermore, the present invention according to claim 25 is a program recording medium characterized by storing a program for directing a computer to perform all or a part of respective functions in each step of the AV contents transmitting method described in any of the claims 16 through 24. The present invention according to claim 28 is a program recording medium storing a program for directing a computer to perform all or a part of each step of the AV contents receiving method described in either respective functions in the claim 26 or 27.

Industrial Applicability

[0147] As described above, it is clear that the present invention according to claim 1 can provide a data transmitting and receiving method for improving the transmission and reception efficiency by improving the security through the update of a control key and reducing the frequency of the authentication and key exchange process. The present invention according to claim 6 can provide a data transmission apparatus for improving the transmission and reception efficiency by improving the security through the update of a control key and reducing the frequency of the authentication and key exchange process. The present invention according to claim 8 can provide a data reception apparatus for improving the transmission and reception efficiency by improving the security through the update of a control key and reducing the frequency of the authentication and key exchange process. Further, the present invention according to claim 14 can provide a data transmission and reception system for improving the transmission and reception efficiency by improving the security through the update of a control key and reducing the frequency of the authentication and key exchange process. The present invention according to claim 15 can provide a program recording medium stor-

ing a program for directing a computer to perform each function of all or a part of each component provided in each means forming part of the present invention.

[0148] In addition, the present invention can provide an AV contents transmitting method capable of allowing an AV contents reception apparatus which cannot use a first encrypting method to decrypt AV contents when an AV contents transmission apparatus transmits AV contents encrypted in the first encrypting method.

[0149] Furthermore, the present invention can provide an AV contents transmission apparatus capable of allowing an AV contents reception apparatus which cannot use a first encrypting method to decrypt AV contents when an AV contents transmission apparatus transmits AV contents encrypted in the first encrypting method.

[0150] In addition, when the above described AV contents transmitting method is used, and when there is an AV contents reception apparatus which receives and decrypts the AV contents encrypted in the first encrypting method in addition to an AV contents reception apparatus which cannot use the first encrypting method, the present invention can provide an AV contents transmitting method and an AV contents receiving method for allowing the AV contents to be decrypted squently.

[0151] Furthermore, when the aforementioned AV contents transmission apparatus instructs the AV contents reception apparatus which cannot use the first encrypting method to decrypt the AV contents, the present invention can provide another AV contents reception apparatus capable of continuously decrypting the AV contents encrypted in the first encrypting method, in addition to the AV contents reception apparatus mentioned above.

Claims

1. A data transmitting and receiving method in which:

   on a transmission side, encrypted digital data obtained by performing a first encryption process on digital data using a work key, and an encrypted work key obtained by performing a second encryption process on the work key using a control key, are transmitted, and
   on a reception side, the encrypted work key is received and decrypted using the control key obtained by performing an authentication and key exchange process with the transmission side, and the encrypted digital data is received and decrypted using the decrypted work key, thereby obtaining the digital data, characterized in that:
   on said transmission side, the control key is periodically or non-periodically updated, an identifier identifying the control key is assigned for each control key; and
   on said reception side, when a reception process is suspended and then resumed, it is determined whether or not the control key has been updated while the reception process is being suspended by referring to the identifier transmitted from the transmission side, and, when it is determined that the control key has been updated, the authentication and key exchange process is performed again, thereby obtaining the updated control key.

2. The data transmitting and receiving method according to claim 1, characterized in that:

   said reception side requests the transmission side to transmit the identifier when the reception process is suspended and then resumed; and
   said transmission side transmits the identifier when the authentication and key exchange process is performed, and also transmits the identifier in response to the request.

3. The data transmitting and receiving method according to claim 1, characterized in that said transmission side periodically or non-periodically transmits the identifier to said reception side.

4. The data transmitting and receiving method according to claim 3, characterized in that said transmission side periodically or non-periodically updates the work key, and transmits to the reception side the identifier, together with the work key, corresponding to the control key used when the first encryption process is performed on the work key.

5. The data transmitting and receiving method according to any one of claims 1 through 4, characterized in that said transmission side does not update the work key until the authentication and key exchange process is completed on the updated control key after the key encryption means updates the control key.

6. A data transmission apparatus, characterized by comprising:

   encryption means periodically or non-periodically updating/generating a work key, performing a first encryption process on digital data using the work key to convert the digital data into encrypted digital data, and transmitting the encrypted digital data to a data reception apparatus;
   a key encryption means periodically or non-periodically updating/generating a control key, performing a second encryption process on the work key using the control key to convert the work key into encrypted work key, and transmit-

ting the encrypted work key to the data reception apparatus;

a transmission side authentication and key exchange means performing an authentication and key exchange process with the data reception apparatus;

identifier generation means generating an identifier identifying the control key; and

identifier transmission means transmitting the identifier to the data reception apparatus.

7. The data transmission apparatus according to claim 6, characterized in that said encryption means does not update the work key until the authentication and key exchange process is completed on the updated control key after the key encryption means updates the control key.

8. A data reception apparatus, characterized by comprising:

a reception side authentication and key exchange means performing an authentication and key exchange process with a data transmission apparatus;

key restoration means restoring a work key by decrypting an encrypted work key converted by performing a second encryption process on the work key using a control key, said restoring process being performed using the control key obtained through said reception side authentication and key exchange means;

decryption means restoring digital data by decrypting encrypted digital data converted by performing a first encryption process on the digital data using the work key, said decrypting process being performed using the work key restored by said key restoration means; and

identifier recognition means determining whether or not the control key has been updated by referring to an identifier identifying the control key transmitted from said data transmission apparatus at least when a reception process is suspended and then resumed, and, when it is determined that the control key has been updated, instructing said reception side authentication and key exchange means to perform again the authentication and key exchange process to obtain the updated control key.

9. The data reception apparatus according to claim 8, characterized by further comprising:

identifier storage means storing the identifier, in which said identifier recognition means determines whether or not the control key has been updated by comparing a latest identifier transmitted from said data transmission apparatus with the identifier transmitted immediately before the latest identifier and stored in said identifier storage means.

10. The data transmission apparatus according to claim 6 or 7 characterized in that said identifier transmission means transmits the identifier when the authentication and key exchange process is performed, and also transmits the identifier in response to a request from said data reception apparatus.

11. The data reception apparatus according to claim 8 or 9, characterized by further comprising

identifier request means requesting said data transmission apparatus to transmit the identifier when the reception process is suspended and then resumes.

12. The data transmission apparatus according to claim 6 or 7, characterized in that said identifier transmission means periodically or non-periodically transmit the identifier to said data reception apparatus.

13. The data transmission apparatus according to claim 12, characterized in that said identifier transmission means transmits to said data reception apparatus the identifier corresponding to the control key used when the second encryption process is performed on the updated/generated work key each time the work key is updated/generated.

14. A data transmission and reception system, characterized by comprising:

a data transmission apparatus according to any one of claims 6, 7, 12, and 13, and a data reception apparatus according to claim 8 or 9; or

a data transmission apparatus according to claim 10, and a data reception apparatus according to claim 11.

15. A computer readable program recording medium, characterized by storing a program for directing a computer to perform each function of all or a part of each component of the data transmission apparatus or the data reception apparatus according to any one of claims 6 through 13.

16. An AV contents transmitting method, characterized by comprising the step of:

encrypting and transmitting AV contents in a second encryption method which can be used

by an AV contents reception apparatus which cannot use a first encrypting method and issues an authentication request when an AV contents transmission apparatus transmits the AV contents encrypted in the first encrypting method using a transmission line.

17. The AV contents transmitting method according to claim 16, characterized in that when the authentication request is issued, and when there is an AV contents reception apparatus which receives and decrypts AV contents encrypted in the first encrypting method in addition to an AV contents reception apparatus which has issued the authentication request, the AV contents reception apparatus which receives and decrypts the AV contents in the first encrypting method is notified that an encrypting method is switched into the second encrypting method.

18. The AV contents transmitting method according to claim 17, characterized in that a notification of switching the encrypting method is given in a predetermined command or is added to the AV contents.

19. The AV contents transmitting method according to claim 18, characterized in that information about what encrypting method is used as the second encrypting method after the switch is given in a predetermined command or is added to the AV contents.

20. The AV contents transmitting method according to claim 18, characterized in that an encryption key or a seed of the encryption key used in the second encrypting method after the switch is given in a predetermined command or is added to the AV contents.

21. The AV contents transmitting method according to claim 16, characterized in that a switching timing of the encrypting method is an updating timing for an encryption key in the first encrypting method used before the authentication request is issued.

22. The AV contents transmitting method according to claim 17, characterized in that a notification that the encrypting method is to be switched into the second encrypting method, and information about a switching timing of the encrypting method are transmitted to at least the AV contents reception apparatus which receives and decrypts the AV contents encrypted in the first encrypting method.

23. The AV contents transmitting method according to claim 16, characterized in that:

said AV contents transmission apparatus stores an AV contents reception apparatus which issued the authentication request; and

it is determined whether or not a command requesting an encryption key for decryption of the AV contents or a seed of the encryption key is received from the AV contents reception apparatus, and when the command is not received, the encrypting method is switched from the second encrypting method to the first encrypting method.

24. The AV contents transmitting method according to claim 16, characterized in that:

said AV contents transmission apparatus checks the encrypting method available by each of the AV contents reception apparatus which issued the authentication request and the other AV contents reception apparatus; and when an AV contents reception apparatus transmitting a command requesting an encryption key for decryption of the AV contents and the seed of the encryption key is an AV contents reception apparatus capable of using the first encrypting method, the encrypting method is switched from the second encrypting method to the first encrypting method.

25. A program recording medium, characterized by storing a program for directing a computer to perform each function of all or a part of each step of the AV contents transmitting method according to any one of claims 16 through 24.

26. An AV contents receiving method, characterized by comprising the steps of:

receiving AV contents transmitted from the AV contents transmitting method according to any one of claims 16 through 24; and
decrypting the encrypted AV contents, based on an encrypting method used when the AV contents are encrypted and using an encryption key used in the encrypting method or a seed of the encryption key.

27. The AV contents receiving method according to claim 26, characterized in that:

there is information about switching the encrypting method transmitted together with or in the AV contents in the AV contents transmitting method according to any one of claims 16 through 24; and
when the information contains none or one of the information about what encrypting method is used after the switch, and the encryption key

used in the encrypting method or a seed of the encryption key,

the information about what encrypting method is used after the switch, or the encryption key used in the encrypting method or a seed of the encryption key, whichever is not contained in the information relating to the switch of the encrypting method, is to be transmitted to the AV contents transmission apparatus.

28. A program recording medium, characterized by storing a program for directing a computer to perform each function of all or a part of each step of the AV contents receiving method according to claim 26 or 27.

29. An AV contents transmission apparatus, characterized by comprising:

encrypting method selection means selecting an encrypting method used when AV contents to be transmitted are encrypted;

encryption key generation means generating an encryption key for encrypting AV contents corresponding to the encrypting method selected by said encrypting method selection means;

encryption means receiving AV contents, also receiving the encryption key from the encryption key generation means, and encrypting the AV contents; and

a transmission side authentication and key exchange means performing an authentication and key exchange process with an AV contents reception apparatus, wherein

when the AV contents reception apparatus is transmitting the AV contents encrypted in the first encrypting method selected by said encrypting method selection means, and when the AV contents reception apparatus which cannot use the first encrypting method issues an authentication request, the transmission side authentication and key exchange means performs an authentication process with the AV contents reception apparatus which issued the authentication request, and

said encrypting method selection means switches the encrypting method into the second encrypting method the AV contents reception apparatus which issued the authentication request can use.

30. The AV contents transmission apparatus according to claim 29, characterized by further comprising an encrypting method notification means issues a notification that the encrypting method is switched into the second encrypting method to an AV contents reception apparatus which is provided in addition to the AV contents reception apparatus which issues an authentication request, and receives and decrypts the AV contents encrypted in the first encrypting method.

31. The AV contents transmission apparatus according to claim 29, characterized in that;

said encryption key generation means periodically or non-periodically updates the encryption key;

said encrypting method selection means switches the encrypting method into the second encrypting method at a timing of said encryption key generation means updating the encryption key in the first encrypting method.

32. The AV contents transmission apparatus according to claim 29, characterized in that

said transmission side authentication and key exchange means stores an AV contents reception apparatus which issued the authentication request, and

it is determined whether or not a command requesting an encryption key for decryption of the AV contents or a seed of the encryption key is received from the AV contents reception apparatus; and

when the command is not received, said encryption key generation means switches the encrypting method from the second encrypting method to the first encrypting method.

33. The AV contents transmission method according to claim 29, characterized in that:

said transmission side authentication and key exchange means checks the encrypting method available by each of the AV contents reception apparatus which issued the authentication request and the other AV contents reception apparatus; and

when an AV contents reception apparatus transmitting a command requesting an encryption key for decryption of the AV contents and the seed of the encryption key is an AV contents reception apparatus capable of using the first encrypting method, said encryption key generation means switches the encrypting method from the second encrypting method to the first encrypting method.

34. The AV contents reception apparatus according to any one of claims 29 through 33, characterized by further comprising:

a reception side authentication and key

exchange means performing an authentication and key exchange process with said AV contents reception apparatus;

encrypting method storage means receiving and information about an encrypting method used in encrypting AV contents from said AV contents transmission apparatus; and

decryption means receiving encrypted AV contents from the AV contents transmission apparatus, receiving an encryption key or a seed of the encryption key from said AV contents transmission apparatus, and decrypting the encrypted AV contents using the encryption key of the seed of the encryption key based on the encrypting method stored in said encrypting method storage means.

35. The AV contents reception apparatus according to claim 34, characterized by further comprising:

request means requesting transmitting information such that;

there is information about switching the encrypting method transmitted together with or in the AV contents from the AV contents transmission apparatus according to any one of claims 29 through 33, and

when the information contains none or one of the information about what encrypting method is used after the switch, and the encryption key used in the encrypting method or a seed of the encryption key,

the information about what encrypting method is used after the switch, or the encryption key used in the encrypting method or a seed of the encryption key, whichever is not contained in the information is to be transmitted.

Amended claims under Art. 19.1 PCT

36. (Added) A data transmission and reception method, characterized in that:

on a transmission side, encrypted digital data obtained by performing an encryption process on digital data using a work key is transmitted;

on a reception side, a control key required to obtain the work key is obtained by performing an authentication and key exchange process with said transmission side, and the received encrypted digital data is decrypted using the work key obtained using the control key to obtain the digital data, characterized in that:

said transmission side periodically and non-periodically updates the control key, assigns an identifier identifying the control, key for each control key, said reception side determines whether or not the control key has been updated while the reception process is suspended by referring to the identifier transmitted from the transmission side when the reception process is suspended and then resumed, and, when it is determined that the control key has been updated, obtains the updated control key by performing again the authentication and key exchange process.

37. (Added) A data transmission apparatus, characterized by comprising:

encryption means performing an encrypting process on digital data using a work key, converting the data into encrypted digital data, and transmitting a result to a data reception apparatus;

control key update/generation means periodically or non-periodically updating/generating a control key required to obtain the work key;

a transmission side authentication and key exchange means performing an authentication and key exchange process with said data reception apparatus;

identifier generation means generating an identifier identifying the control key; and

identifier transmission means transmitting the identifier to said data reception apparatus.

38. (Added) A data reception apparatus, characterized by comprising:

reception means receiving encrypted digital data obtained by encrypting digital data using a work key;

a reception side authentication and key exchange means performing an authentication and key exchange process with a data transmission apparatus;

a control key obtaining means obtaining a control key required to obtain the work key through the reception side authentication and key exchange means;

decryption means decrypting the encrypted digital data using the work key generated using the control key to restoring the digital data; and

identifier recognition means determining whether or not the control key has been updated by referring to an identifier identifying the control key transmitted from the data transmission apparatus when the receiving process is suspended and then resumed, and, when it is determined that the control key has been updated, the updated control key is obtained by performing again the authentication and key exchange process with the reception side authentication and key exchange means.

Fig. 1

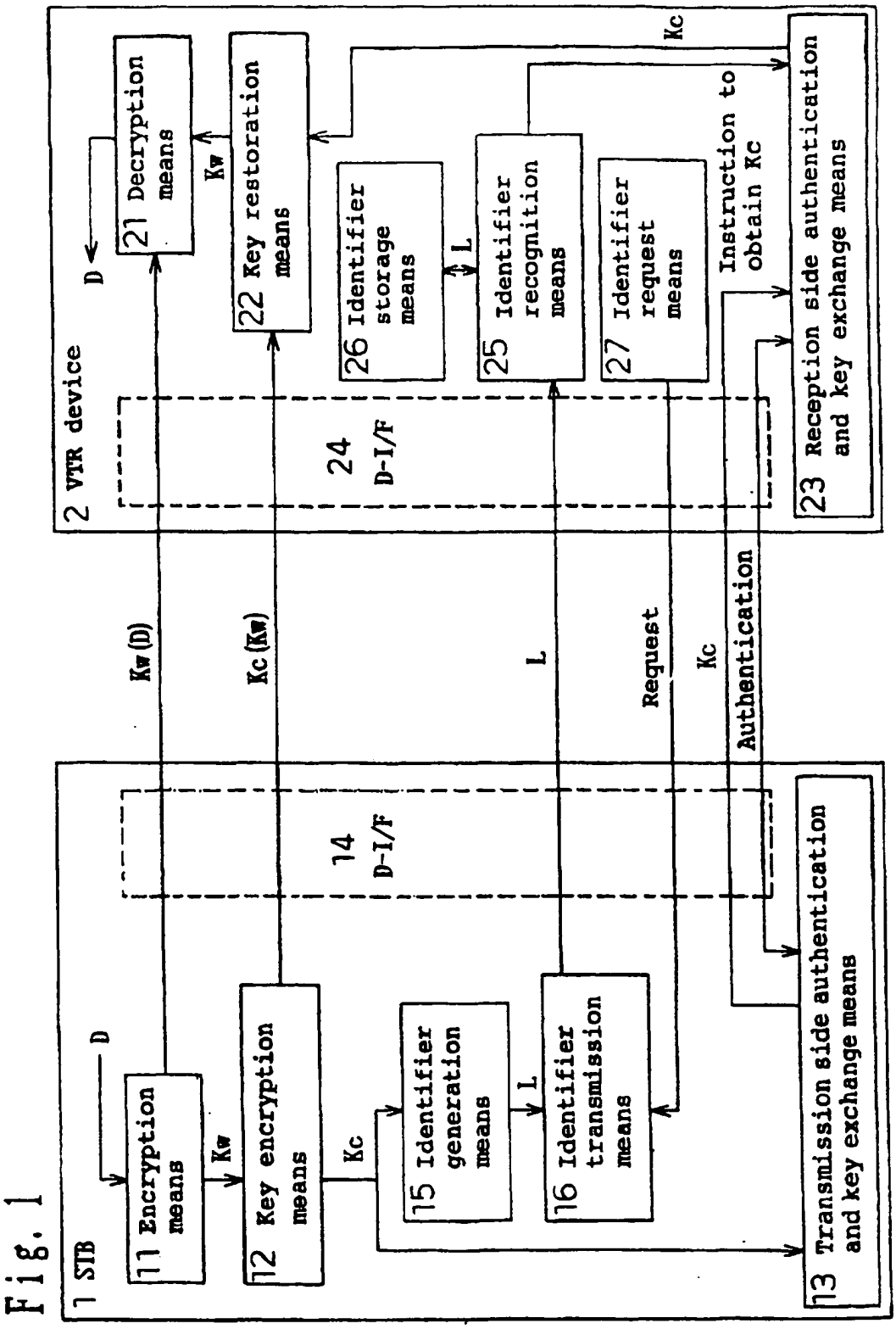

1 STB
11 Encryption means
D
Kw
12 Key encryption means
Kc
15 Identifier generation means
L
16 Identifier transmission means
13 Transmission side authentication and key exchange means
14 D-I/F
Kw(D)
Kc(Kw)
L
Request
Kc
Authentication
2 VTR device
21 Decryption means
D
Kw
22 Key restoration means
Kc
26 Identifier storage means
L
25 Identifier recognition means
27 Identifier request means
Instruction to obtain Kc
24 D-I/F
23 Reception side authentication and key exchange means

Fig. 2

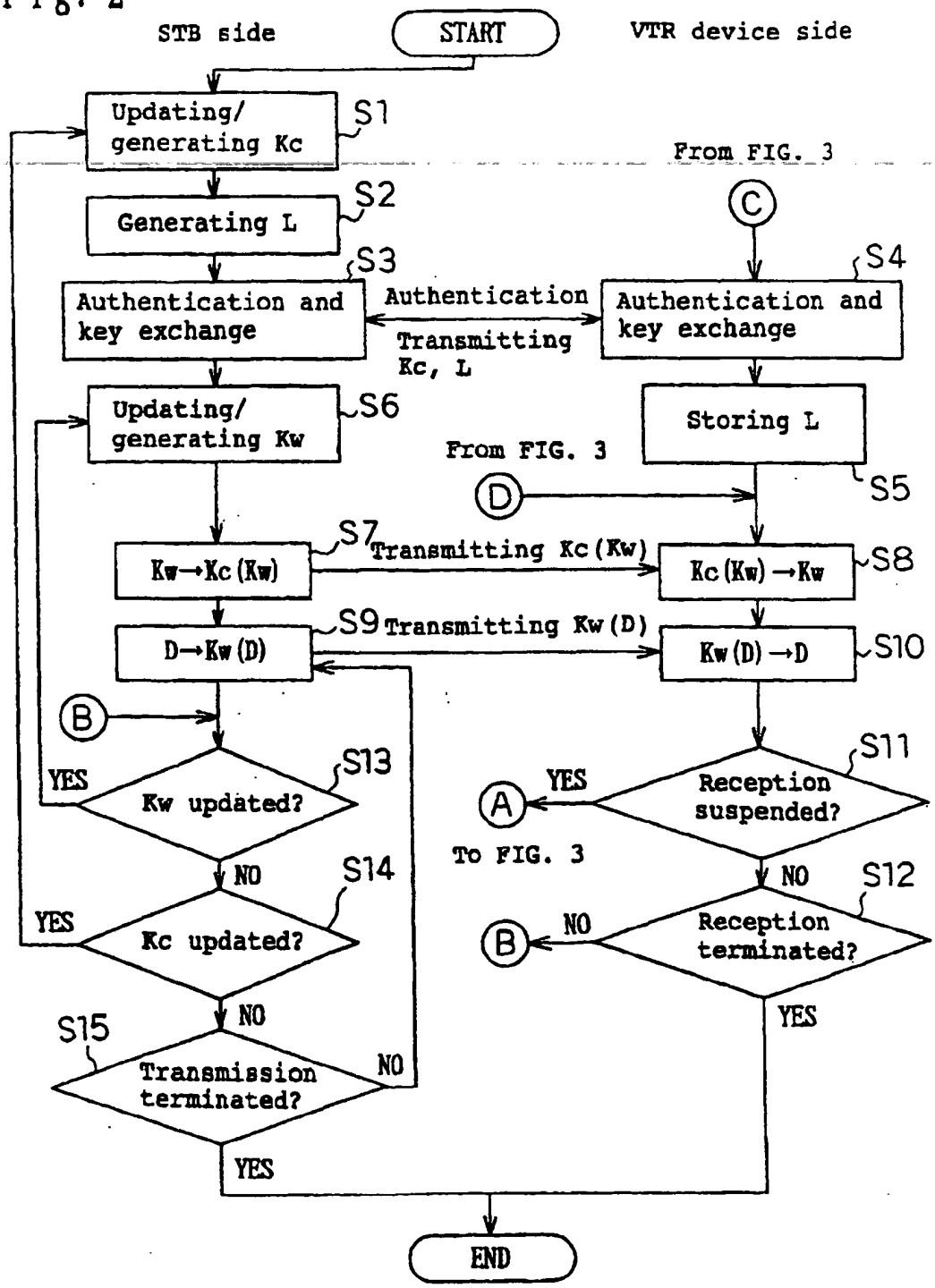

STB side
START
VTR device side
Updating/ generating Kc
S1
From FIG. 3
Generating L
S2
C
S3
S4
Authentication and key exchange
Authentication
Transmitting Kc, L
Authentication and key exchange
Updating/ generating Kw
S6
Storing L
From FIG. 3
D
S5
S7
Transmitting Kc(Kw)
Kw→Kc(Kw)
Kc(Kw)→Kw
S8
S9
Transmitting Kw(D)
D→Kw(D)
Kw(D)→D
S10
B
S11
YES
Kw updated?
S13
YES
A
Reception suspended?
To FIG. 3
NO
S14
NO
S12
YES
Kc updated?
B
NO
Reception terminated?
NO
S15
YES
Transmission terminated?
NO
YES
END

Fig. 3

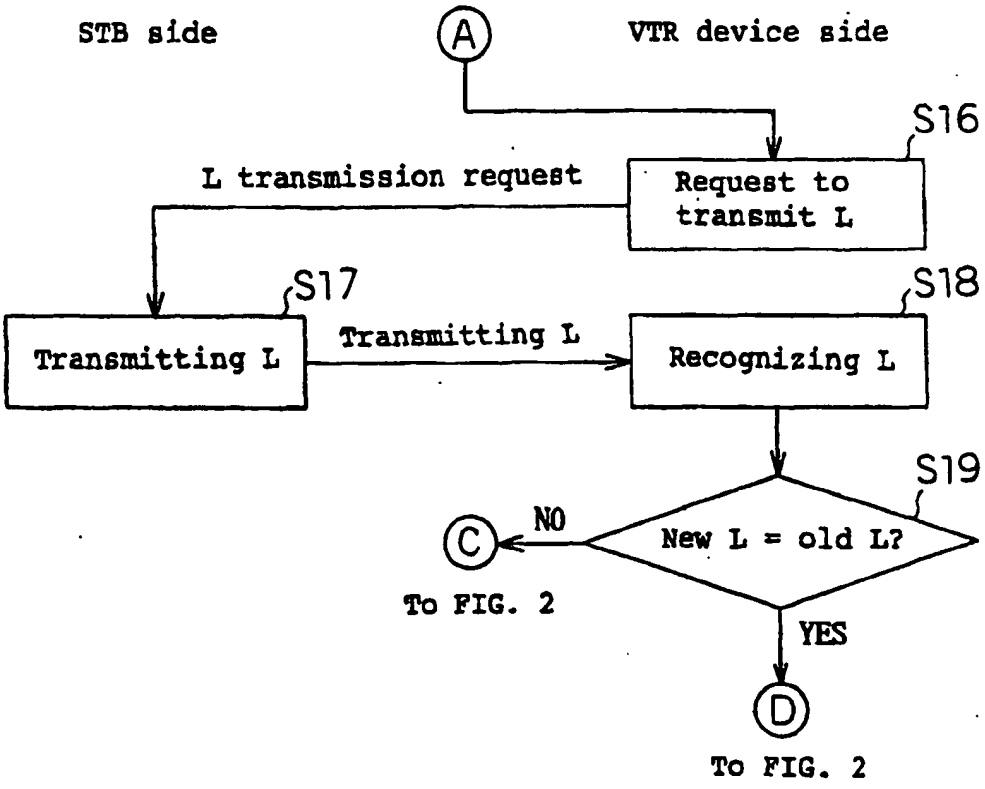

STB side
A
VTR device side
S16
L transmission request
Request to transmit L
S17
S18
Transmitting L
Transmitting L
Recognizing L
S19
NO
C
New L = old L?
To FIG. 2
YES
D
To FIG. 2

Fig. 4

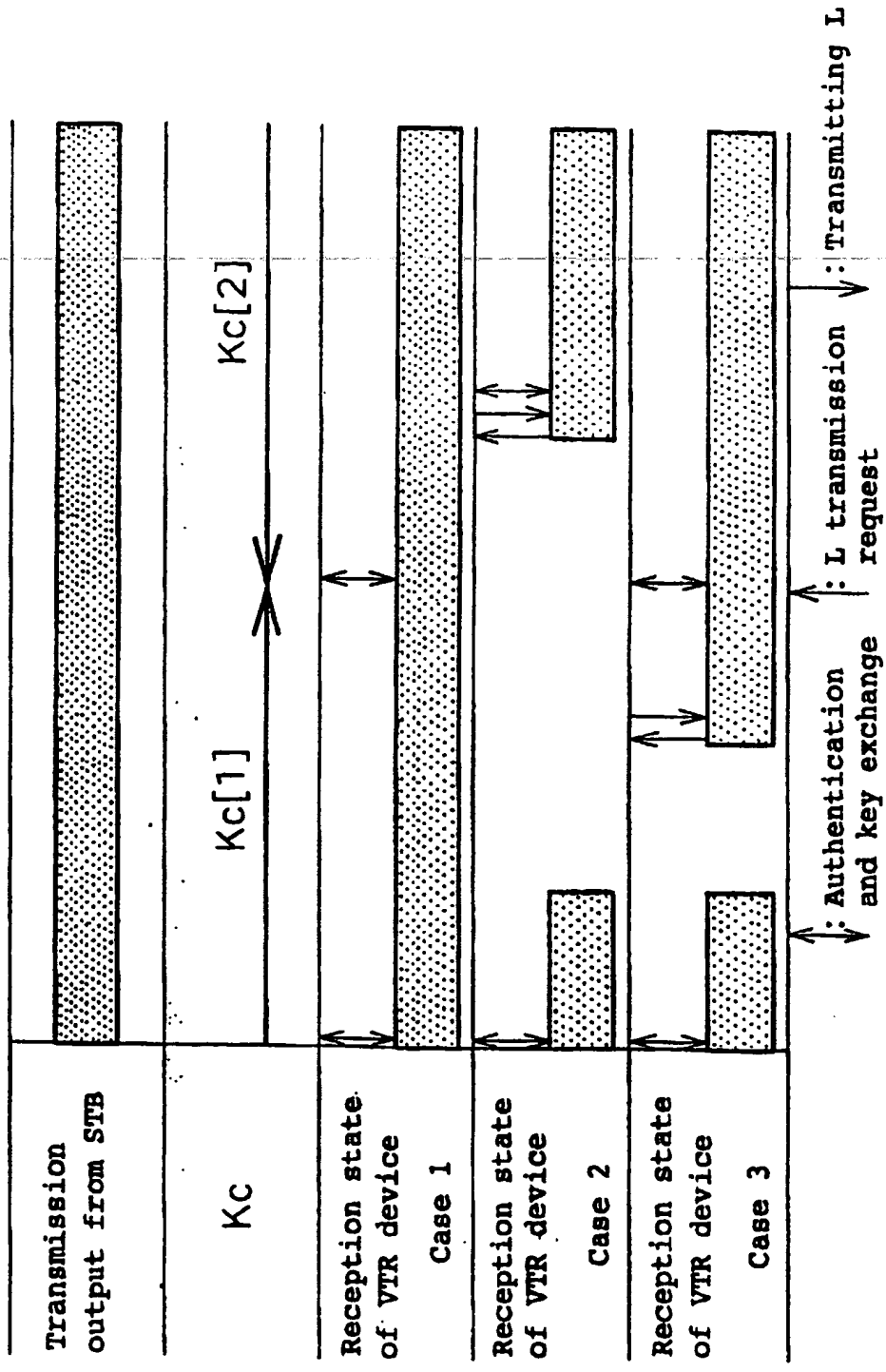

Transmission output from STB
Kc
Kc[1]
Kc[2]
Reception state of VTR device Case 1
Reception state of VTR device Case 2
Reception state of VTR device Case 3
: Authentication and key exchange
: L transmission request
: Transmitting L

Fig. 5

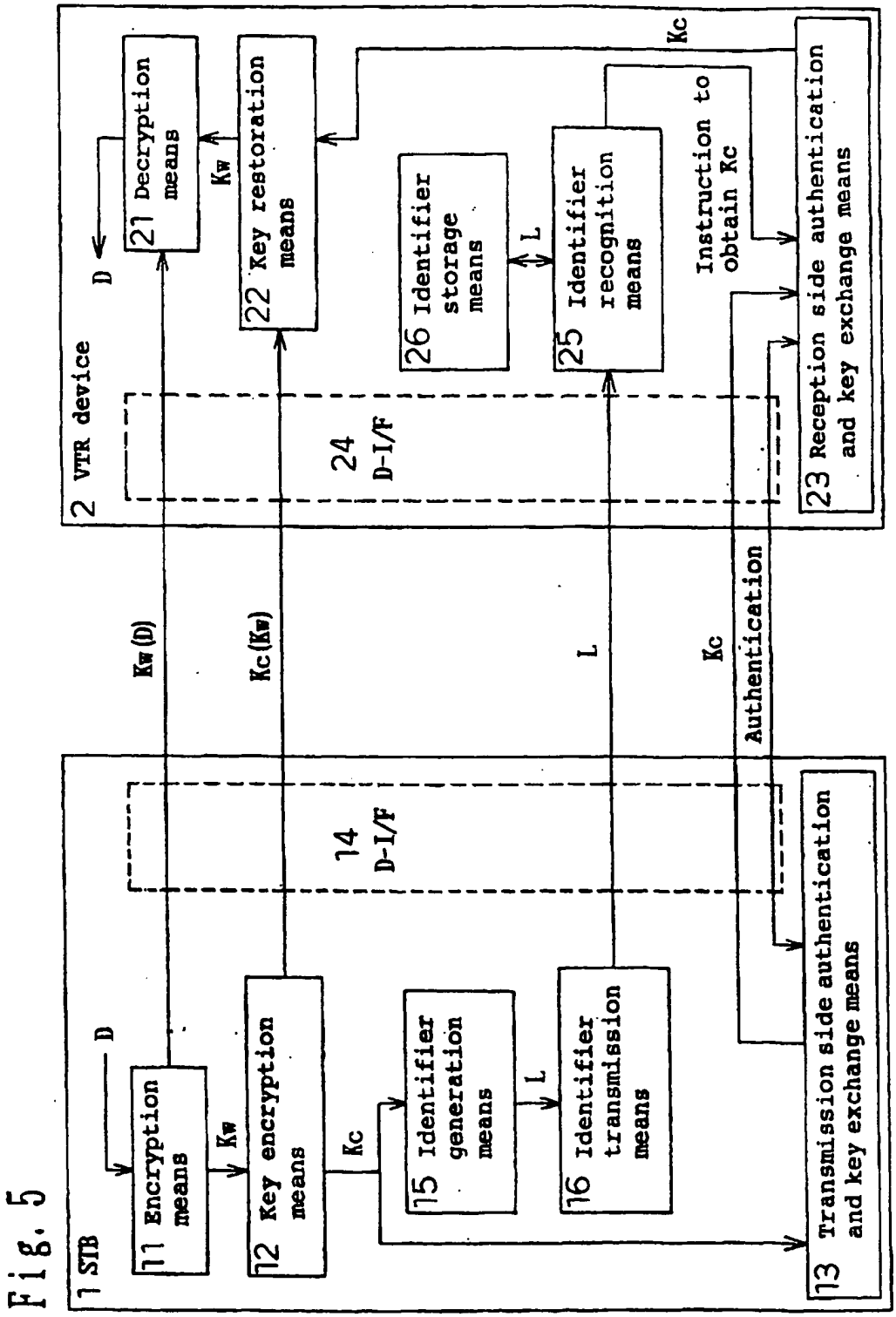

1 STB
11 Encryption means
D
Kw
12 Key encryption means
Kc
15 Identifier generation means
L
16 Identifier transmission means
14 D-I/F
13 Transmission side authentication and key exchange means
Kw(D)
Kc(Kw)
L
Kc
Authentication
2 VTR device
21 Decryption means
D
Kw
22 Key restoration means
24 D-I/F
26 Identifier storage means
L
25 Identifier recognition means
Instruction to obtain Kc
Kc
23 Reception side authentication and key exchange means

Fig. 6

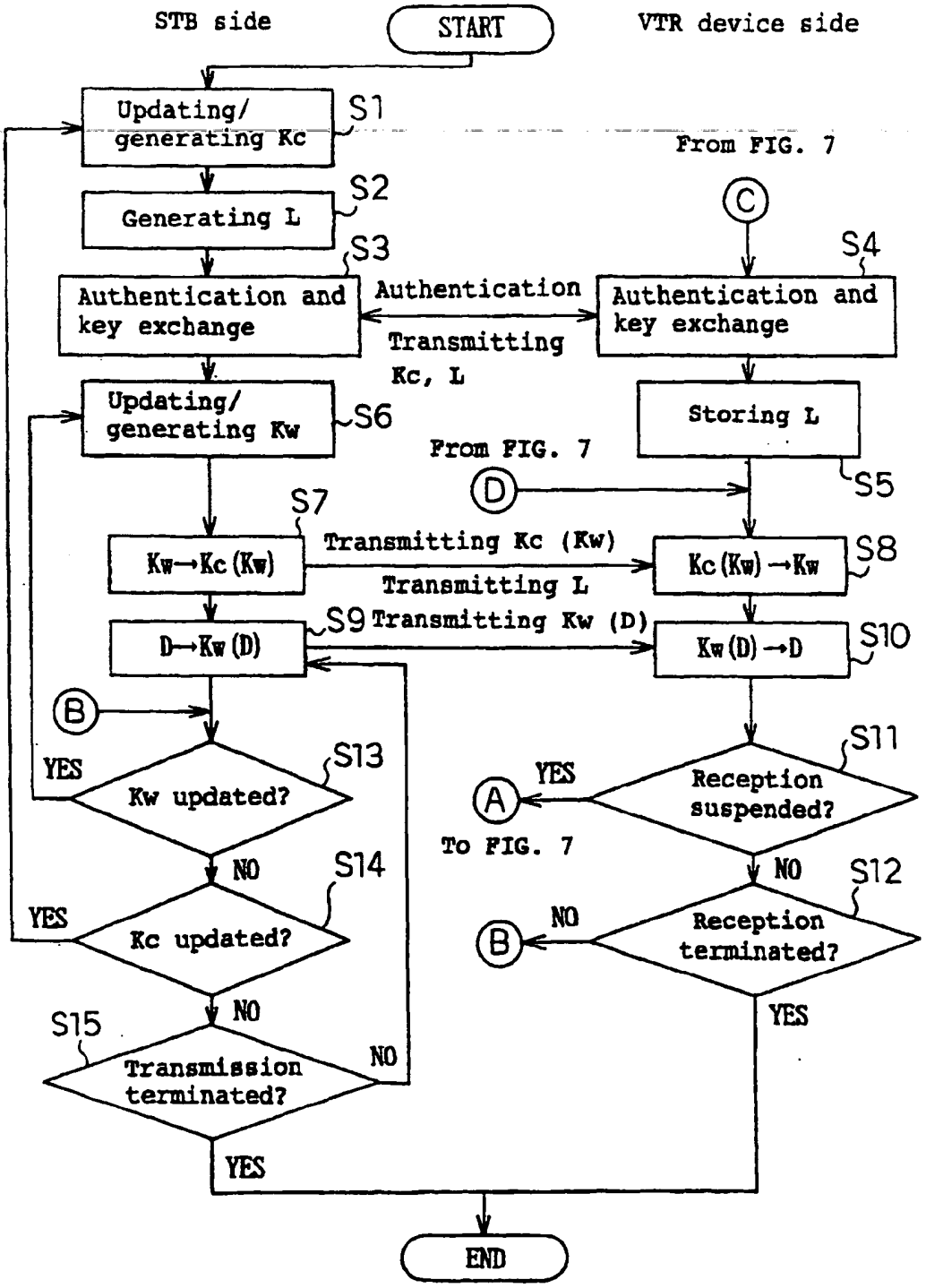

STB side
START
VTR device side
Updating/ generating Kc
S1
From FIG. 7
Generating L
S2
C
S3
S4
Authentication and key exchange
Authentication
Transmitting Kc, L
Authentication and key exchange
Updating/ generating Kw
S6
Storing L
From FIG. 7
D
S5
S7
Kw→Kc (Kw)
Transmitting Kc (Kw)
Transmitting L
Kc (Kw)→Kw
S8
D→Kw (D)
S9
Transmitting Kw (D)
Kw (D)→D
S10
B
S11
YES
Kw updated?
S13
YES
A
Reception suspended?
To FIG. 7
NO
S14
NO
S12
YES
Kc updated?
NO
B
Reception terminated?
S15
NO
Transmission terminated?
NO
YES
YES
END

Fig. 7

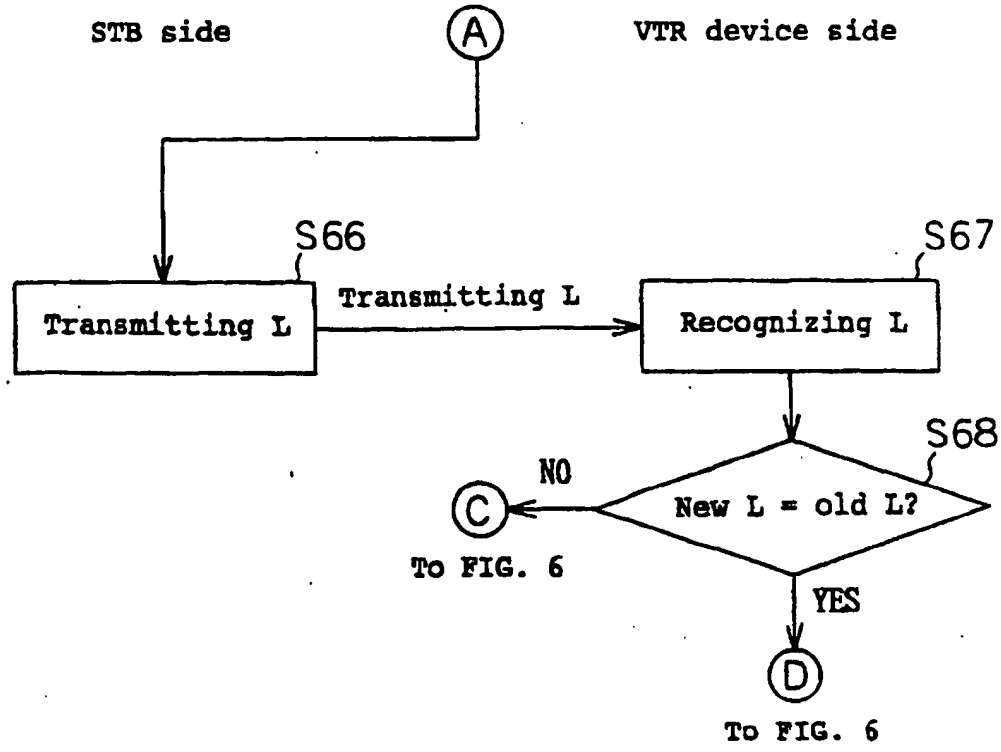

STB side
A
VTR device side
S66
Transmitting L
Transmitting L
S67
Recognizing L
S68
NO
C
New L = old L?
To FIG. 6
YES
D
To FIG. 6

Fig. 8

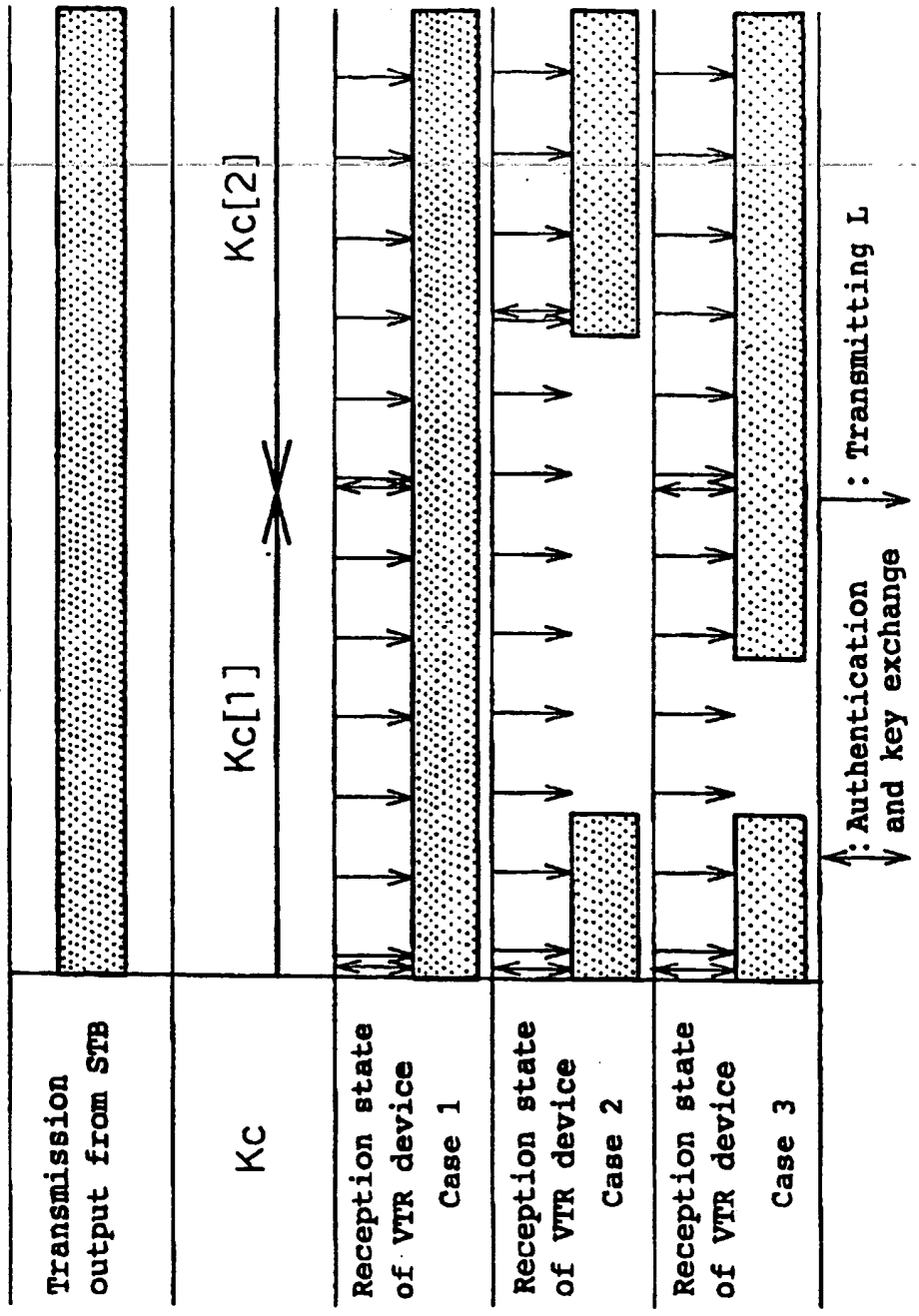

Transmission output from STB
Kc
Kc[1]
Kc[2]
Reception state of VTR device Case 1
Reception state of VTR device Case 2
Reception state of VTR device Case 3
: Authentication and key exchange
: Transmitting L

Fig. 9

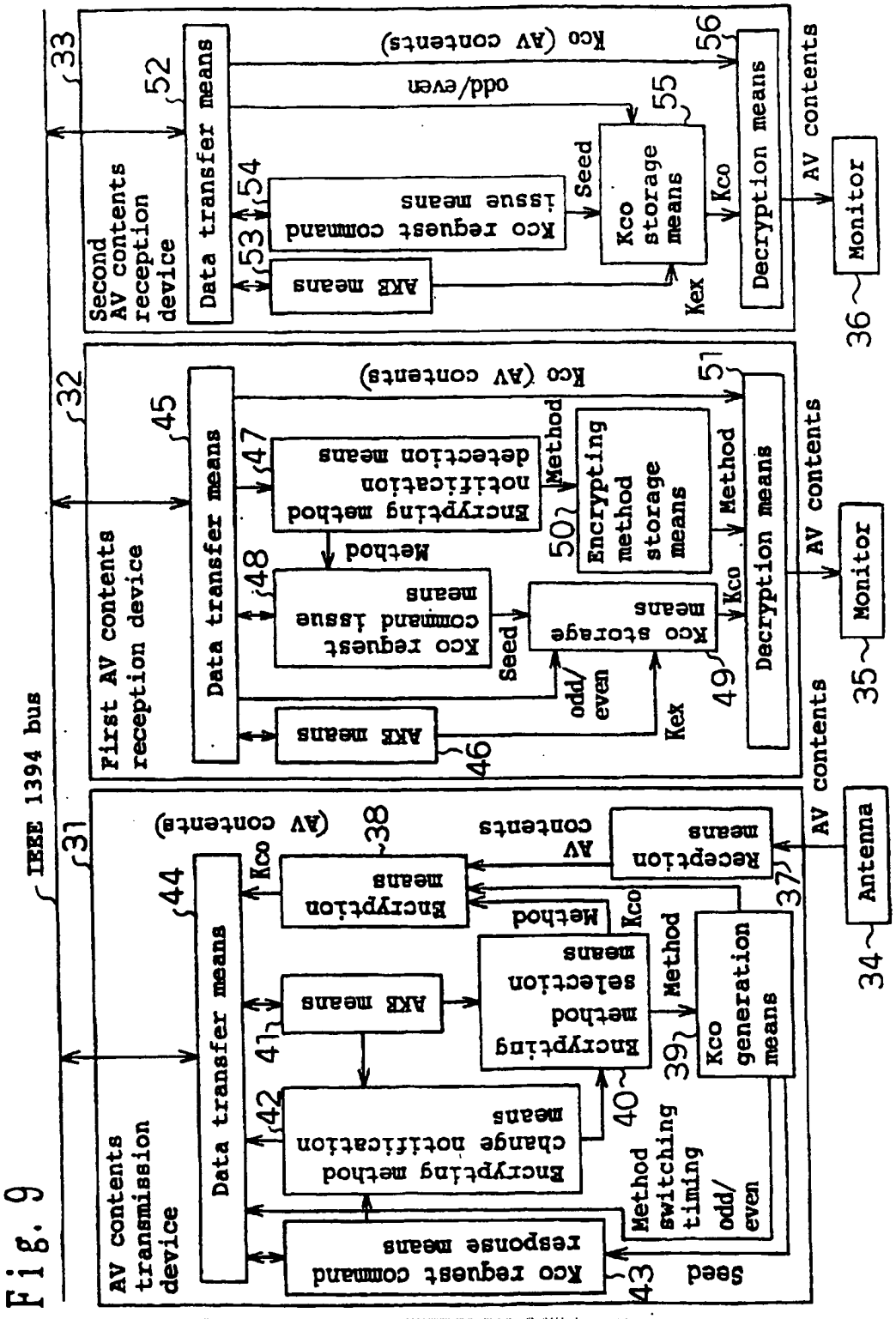

IEEE 1394 bus
AV contents transmission device
Data transfer means
Kco request command response means
Encrypting method change notification means
Encrypting method selection means
Kco generation means
AKE means
Encryption means
Reception means
Antenna
Method switching timing
odd/even
Seed
Kco (AV contents)
AV contents
First AV contents reception device
Kco request command issue means
Kco storage means
Encrypting method notification means
Encrypting method storage means
Decryption means
Monitor
Kex
Second AV contents reception device

Fig. 10 (a)

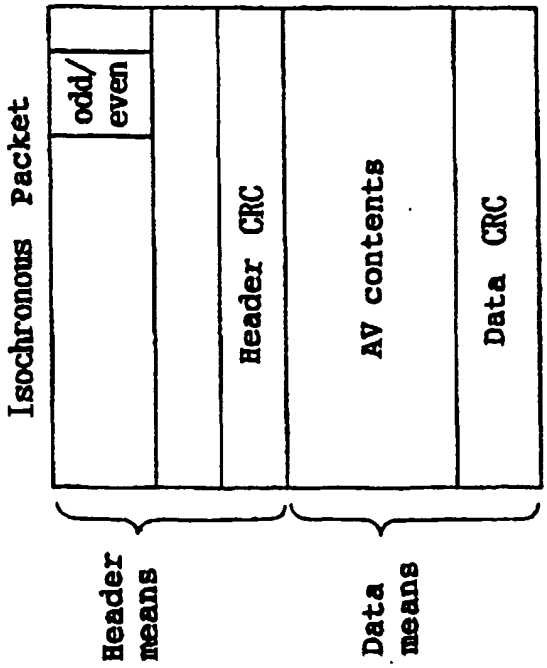


Fig. 10 (b)

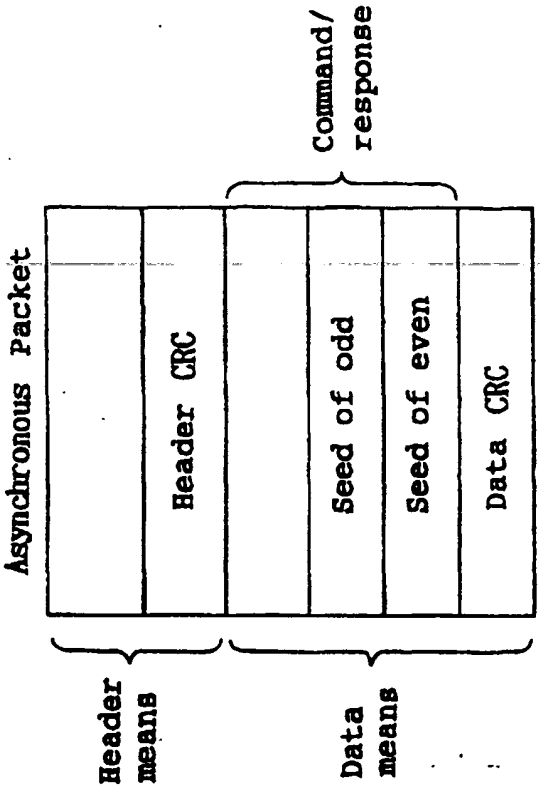


Fig. 11

Operations of AV contents transmission device 31

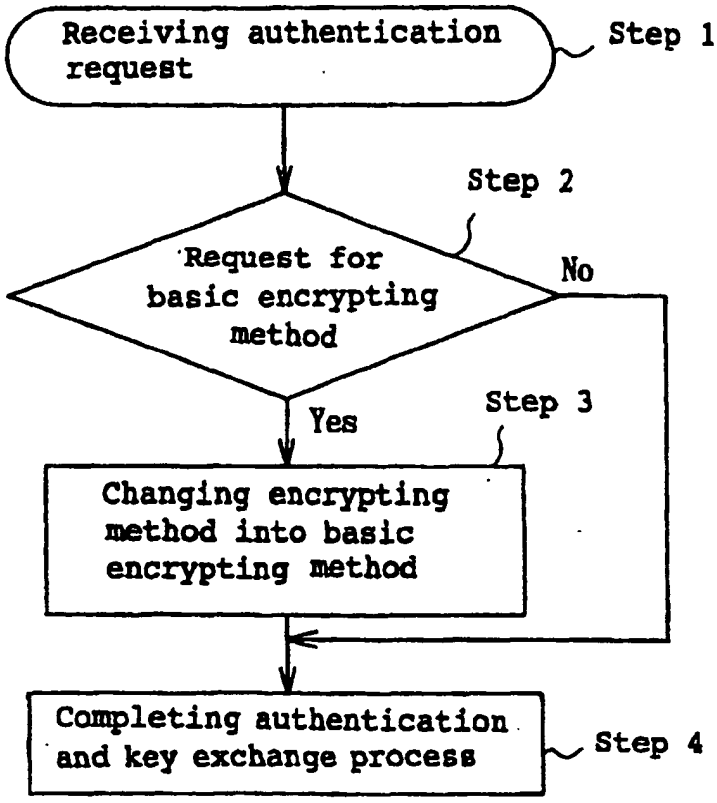


Fig. 12

Operations of first AV contents reception device 32

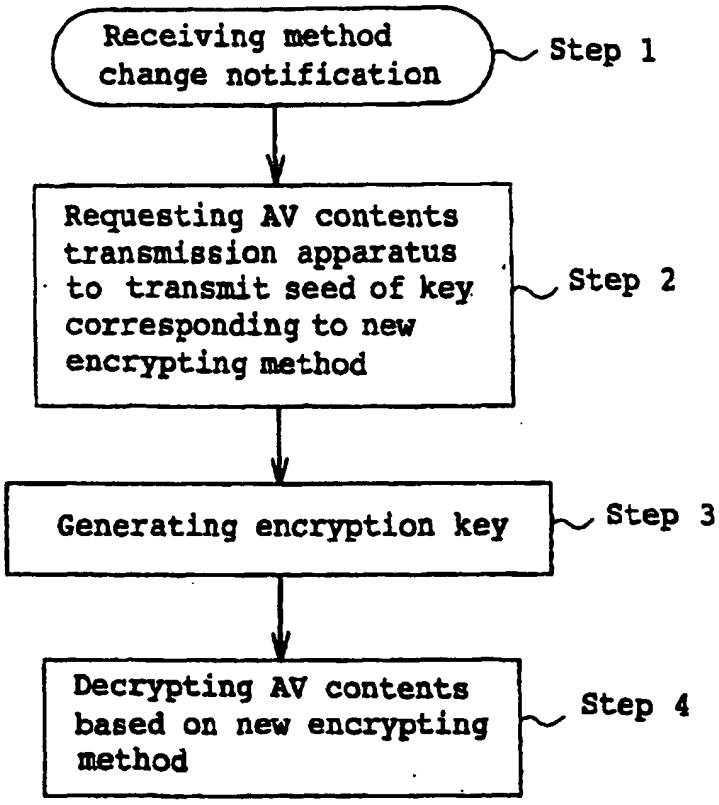


Fig. 13

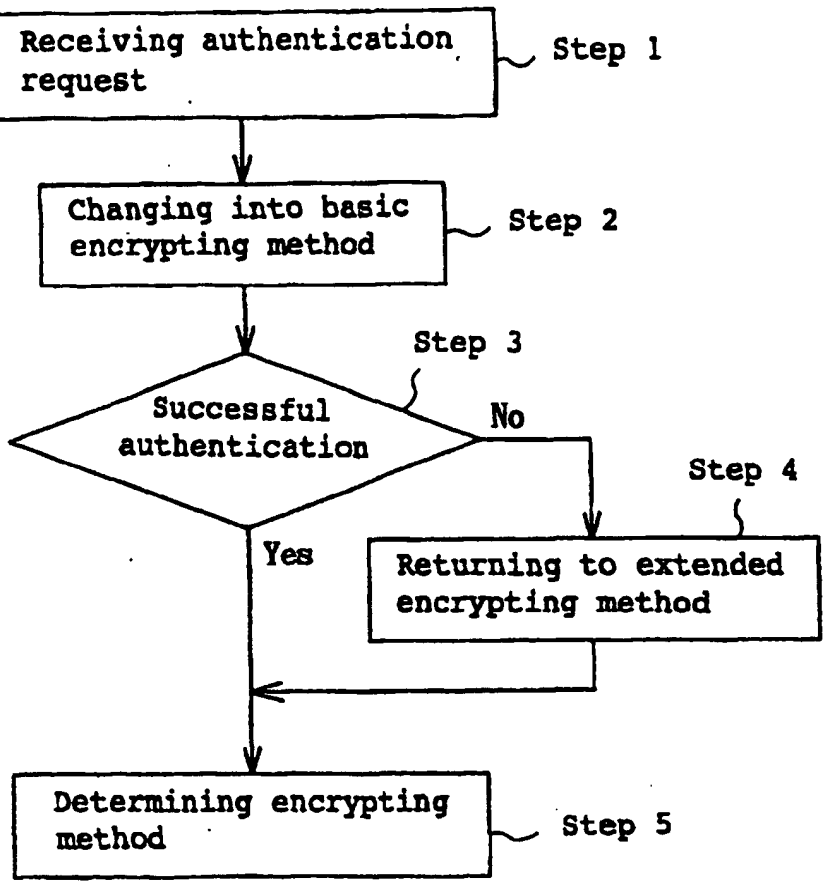

Receiving authentication request
Step 1
Changing into basic encrypting method
Step 2
Step 3
Successful authentication
No
Step 4
Yes
Returning to extended encrypting method
Determining encrypting method
Step 5

Fig. 14

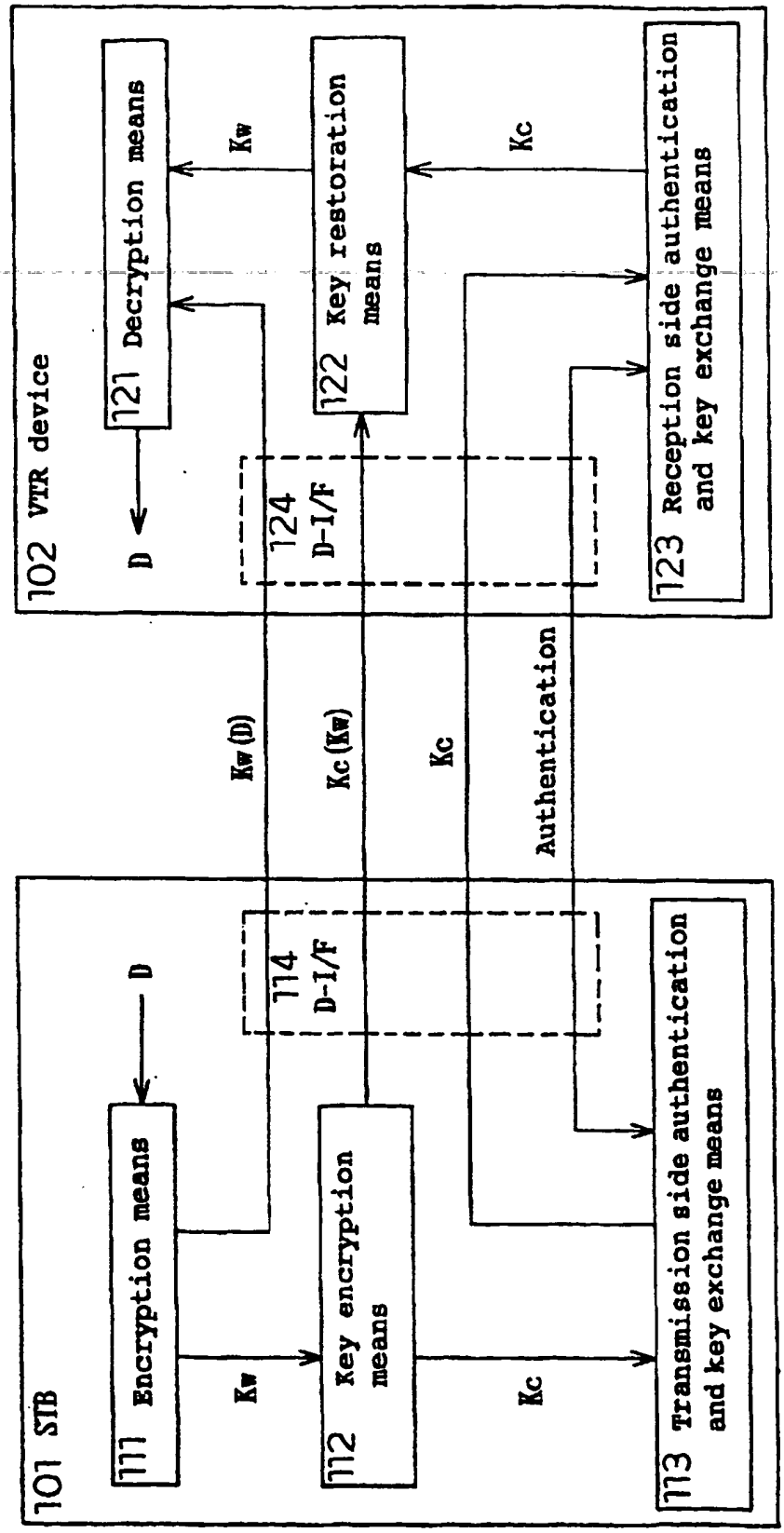
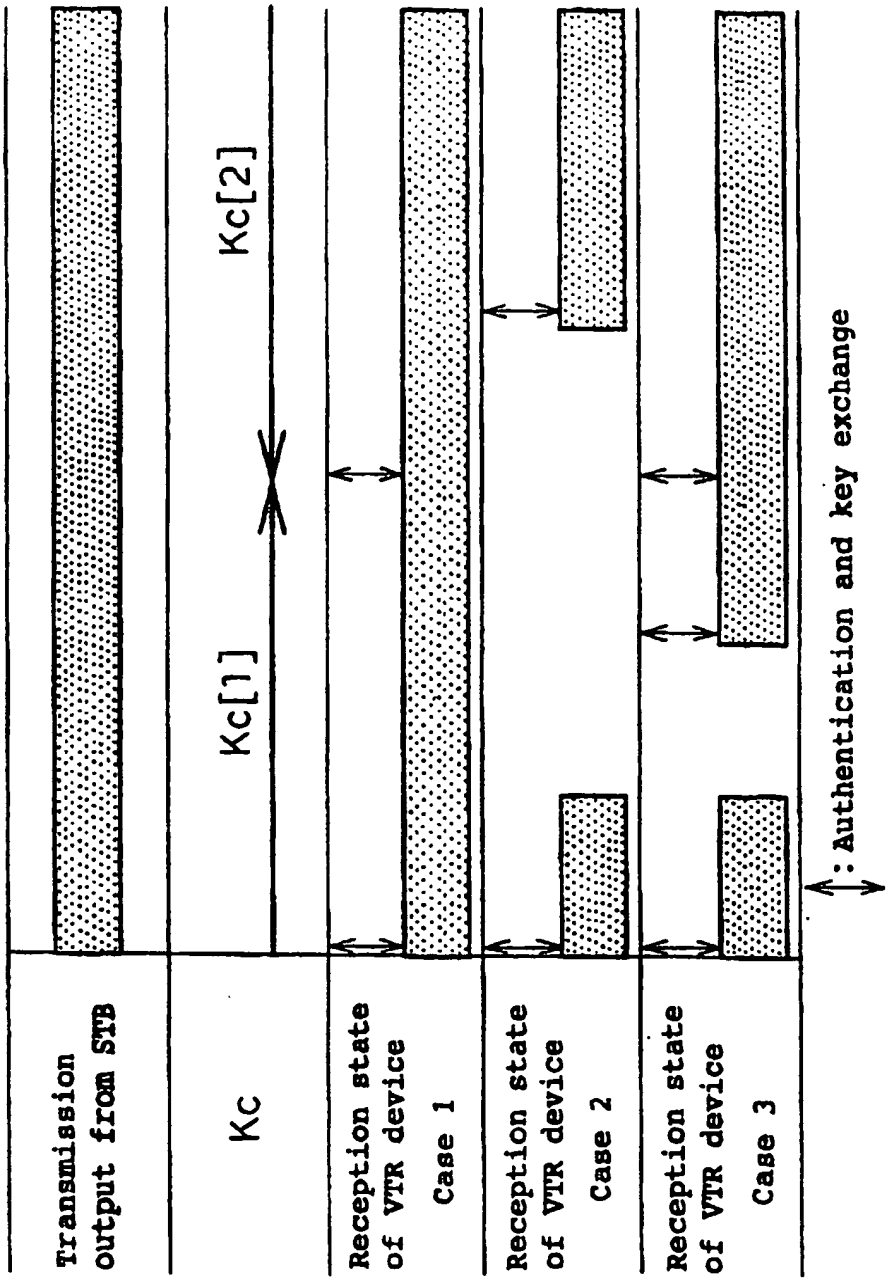

101 STB
111 Encryption means
112 Key encryption means
113 Transmission side authentication and key exchange means
114 D-I/F
D
Kw
Kc
Kw(D)
Kc(Kw)
Kc
Authentication
102 VTR device
121 Decryption means
122 Key restoration means
123 Reception side authentication and key exchange means
124 D-I/F
D
Kw
Kc

Fig. 15


Transmission output from STB
Kc
Kc[1]
Kc[2]
Reception state of VTR device Case 1
Reception state of VTR device Case 2
Reception state of VTR device Case 3
: Authentication and key exchange

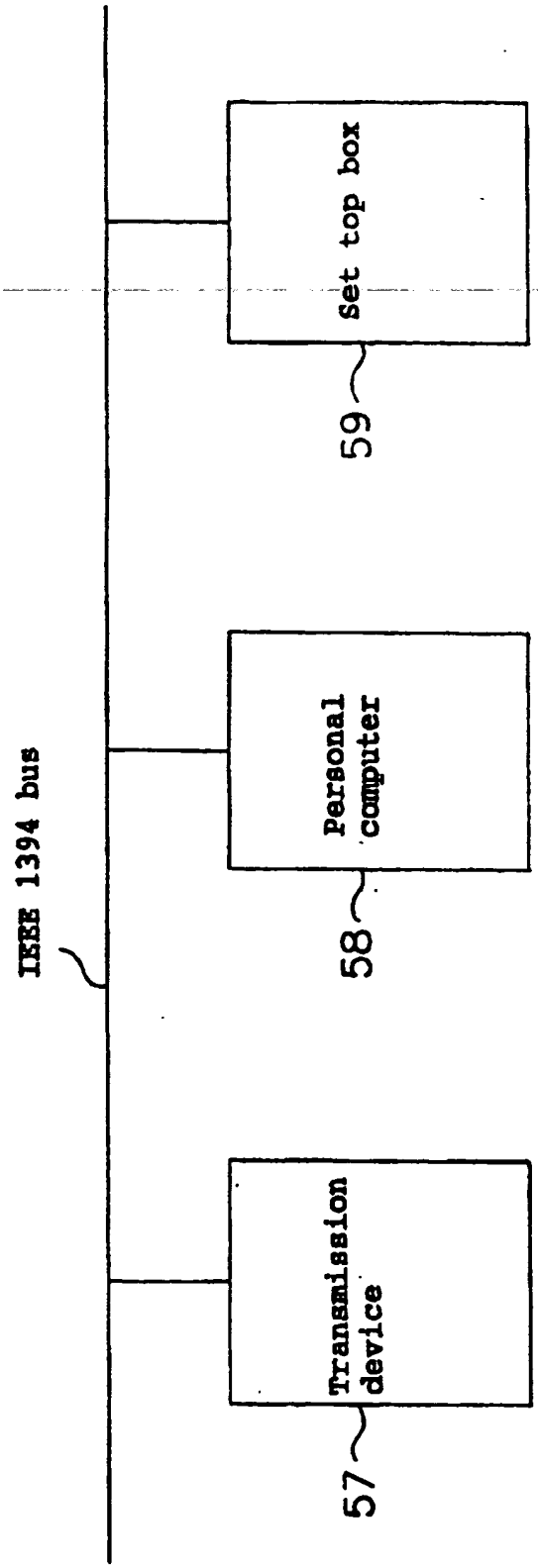

IEEE 1394 bus
Set top box
59
Personal computer
58
Transmission device
57

Fig. 16

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/01606

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[6] H04L9/08, H04L9/14, H04L9/32, H04H1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[6] H04L9/08, H04L9/14, H04L9/32, H04H1/00

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 63-151136, A (NEC Corp.), 23 June, 1988 (23. 06. 88), Full text ; Figs. 1 to 4 (Family: none)	1-15
Y	JP, 9-18468, A (Canon Inc.), 17 January, 1997 (17. 01. 97), Full text ; Figs. 1 to 26 & EP, 751646, A & AU, 9656198, A & JP, 9-16678, A & JP, 9-16679, A & JP, 9-18469, A & JP, 9-46329, A & CA, 2179971, A	16-35

[x] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
13 July, 1999 (13. 07. 99)	21 July, 1999 (21. 07. 99)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/01606

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP, 9-18469, A (Canon Inc.), 17 January, 1997 (17. 01. 97), Page 3, column 3, line 48 to column 4, lines 23, 47 to page 4, column 5, lines 4, 27 to 36 ; page 5, column 7, line 40 to column 8, line 47 ; page 11, column 19, lines 5 to 23 ; Figs. 1 to 17 & EP, 751646, A & AU, 9656198, A & JP, 9-16678, A & JP, 9-16679, A & JP, 9-18468, A & JP, 9-46329, A & CA, 2179971, A	16-35
A	JP, 4-297157, A (Mitsubishi Electric Corp.), 21 October, 1992 (21. 10. 92), Full text ; Figs. 1 to 3 (Family: none)	1-15
A	JP, 59-134939, A (NEC Corp.), 2 August, 1985 (02. 08. 85), Full text ; Figs. 1 to 4 (Family: none)	16-35

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

Fig. 1

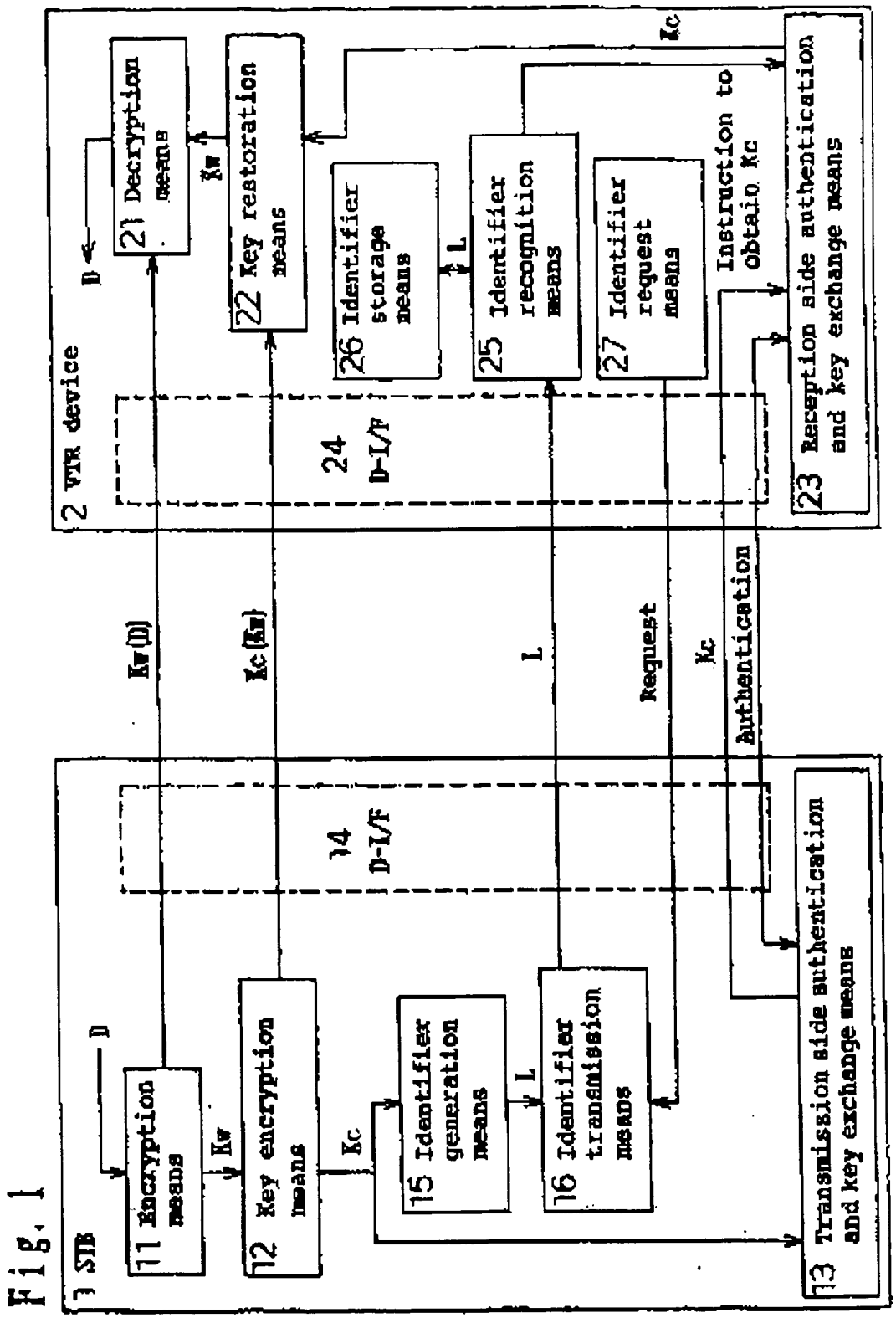

1 STB
11 Encryption means
12 Key encryption means
13 Transmission side authentication and key exchange means
14 D-I/F
15 Identifier generation means
16 Identifier transmission means
2 VTR device
21 Decryption means
22 Key restoration means
23 Reception side authentication and key exchange means
24 D-I/F
25 Identifier recognition means
26 Identifier storage means
27 Identifier request means
Instruction to obtain Kc
D
Kw
Kc
L
Kw(D)
Kc(Kw)
L
Request
Kc
Authentication

Fig. 2

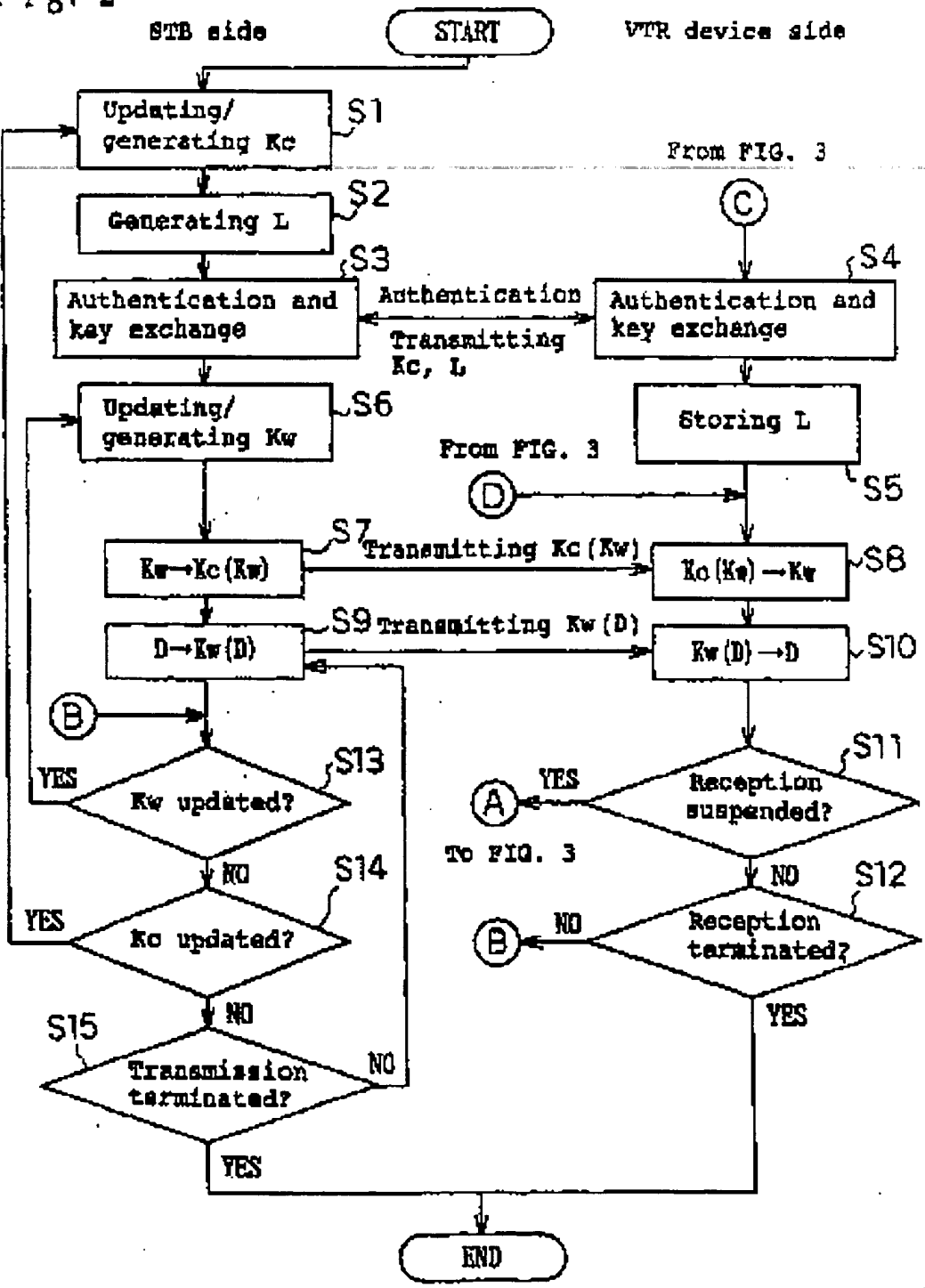

STB side
START
VTR device side
Updating/ generating Kc
S1
From FIG. 3
Generating L
S2
C
S3
S4
Authentication and key exchange
Authentication
Transmitting Kc, L
Authentication and key exchange
Updating/ generating Kw
S6
Storing L
From FIG. 3
D
S5
S7
Transmitting Kc(Kw)
Kw→Kc(Kw)
Kc(Kw)→Kw
S8
D→Kw(D)
S9
Transmitting Kw(D)
Kw(D)→D
S10
B
S11
YES
Kw updated?
S13
A
YES
Reception suspended?
To FIG. 3
NO
S14
NO
S12
YES
Kc updated?
B
NO
Reception terminated?
NO
S15
YES
Transmission terminated?
NO
YES
END

Fig. 3

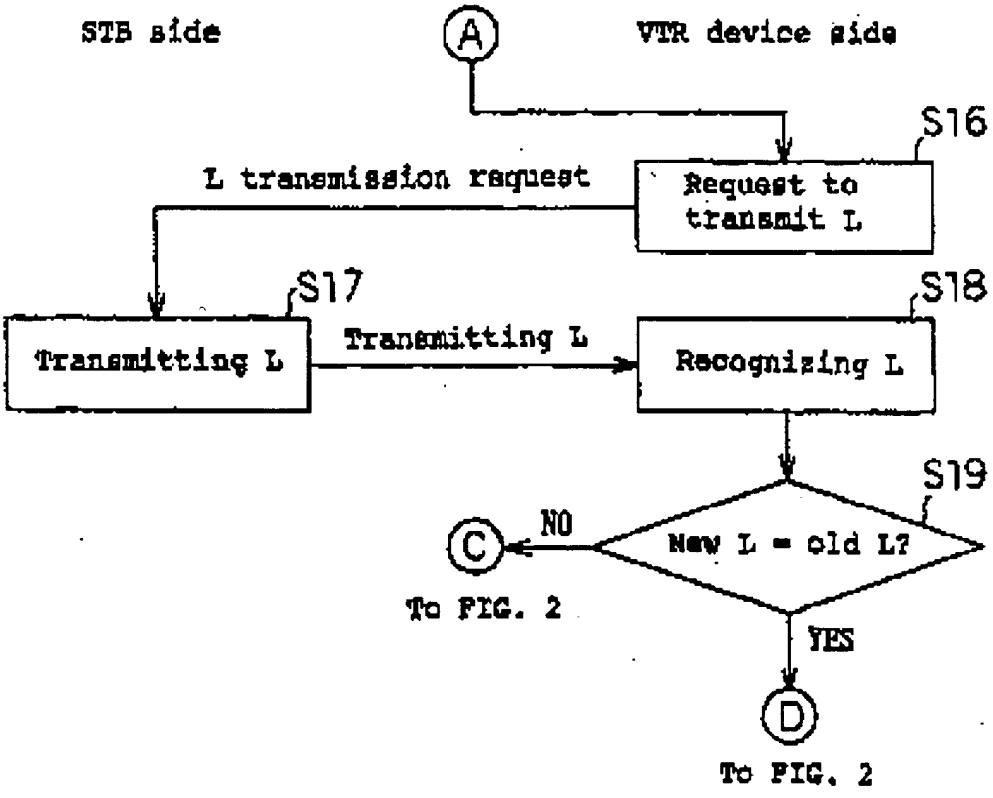

STB side
A
VTR device side
S16
L transmission request
Request to transmit L
S17
S18
Transmitting L
Transmitting L
Recognizing L
S19
NO
New L = old L?
C
To FIG. 2
YES
D
To FIG. 2

Fig. 4

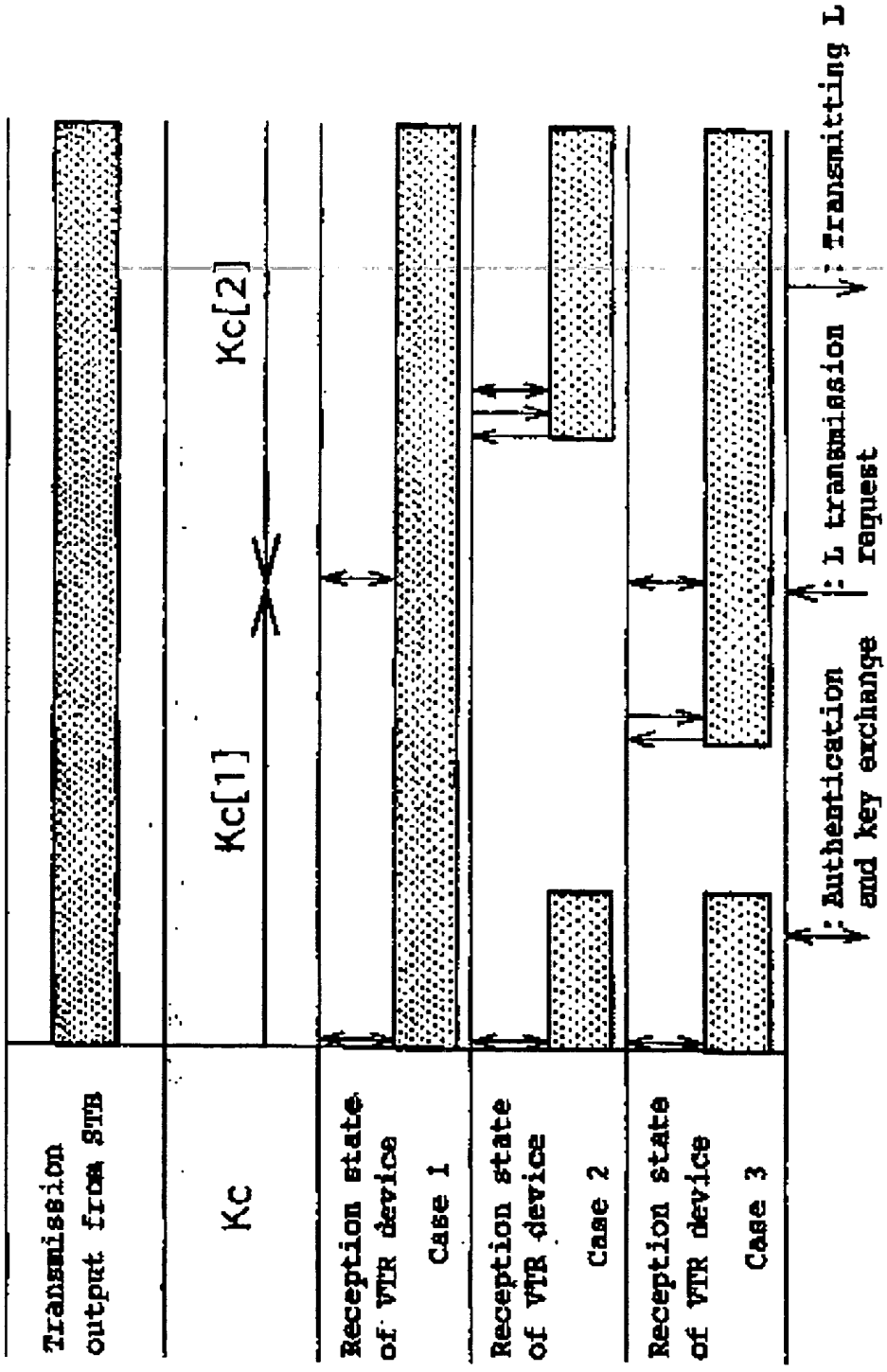

Transmission output from STB
Kc
Kc[1]
Kc[2]
Reception state of VTR device Case 1
Reception state of VTR device Case 2
Reception state of VTR device Case 3
: Authentication and key exchange
: L transmission request
: Transmitting L

Fig. 5

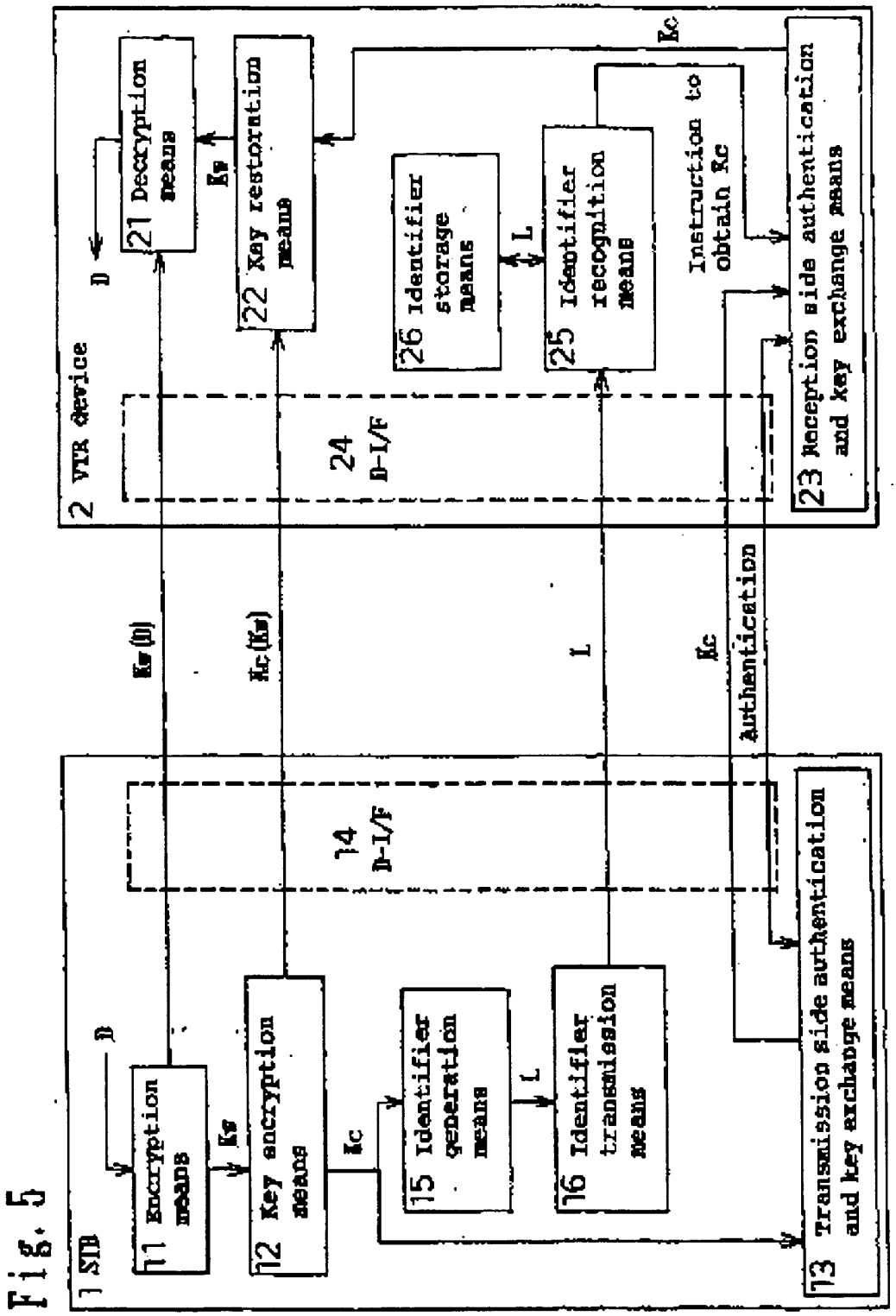

1 STB
D
11 Encryption means
Ks
12 Key encryption means
Kc
15 Identifier generation means
L
16 Identifier transmission means
13 Transmission side authentication and key exchange means
14 D-I/F
Ks(D)
Kc(Ks)
L
Kc
Authentication
2 VTR device
D
21 Decryption means
Ks
22 Key restoration means
26 Identifier storage means
L
25 Identifier recognition means
24 D-I/F
Kc
Instruction to obtain Kc
23 Reception side authentication and key exchange means

Fig. 6

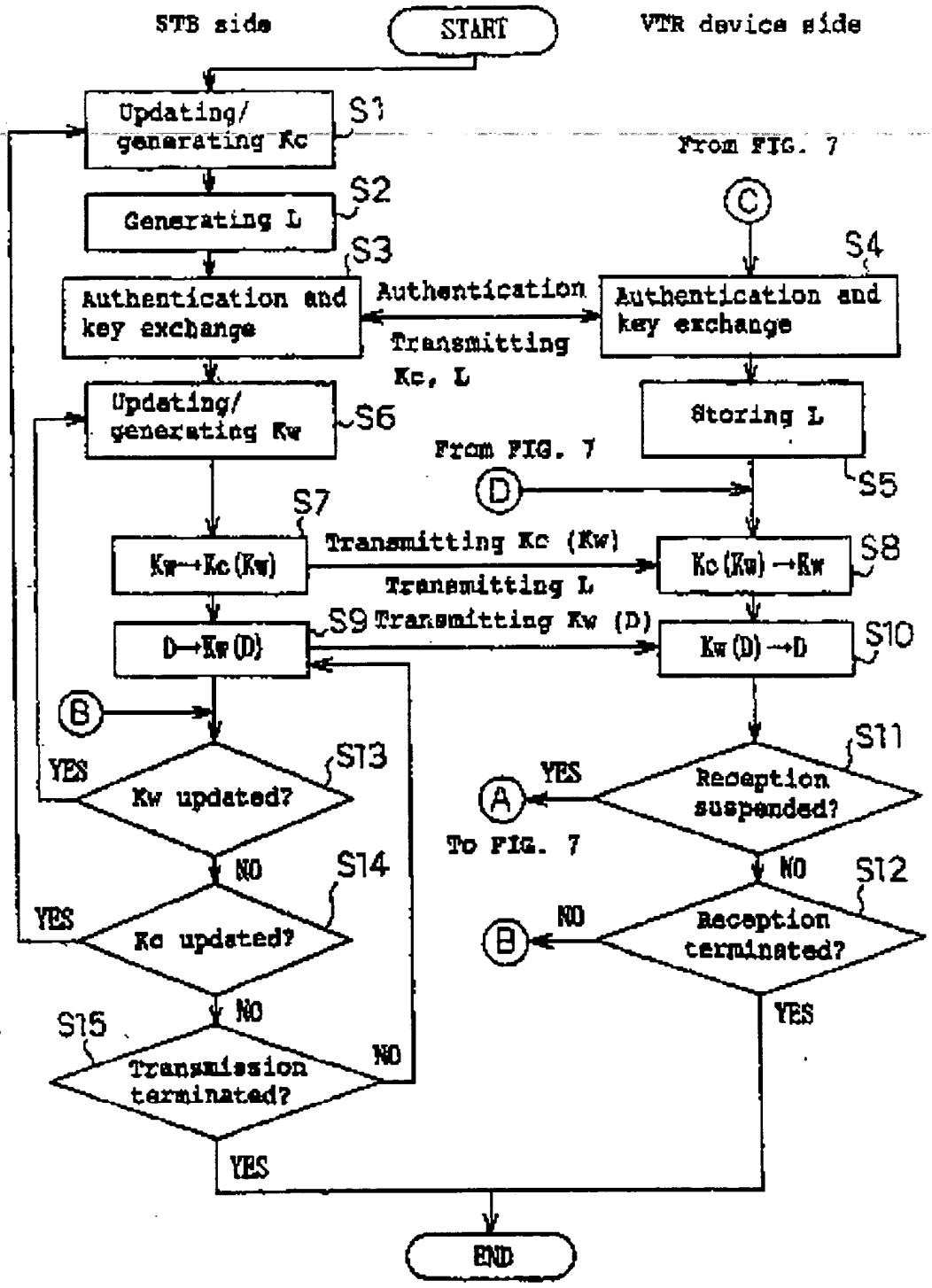

STB side
START
VTR device side
Updating/ generating Kc
S1
From FIG. 7
Generating L
S2
C
S4
S3
Authentication and key exchange
Authentication
Transmitting Kc, L
Authentication and key exchange
Updating/ generating Kw
S6
Storing L
From FIG. 7
D
S5
S7
Kw→Kc(Kw)
Transmitting Kc (Kw)
Transmitting L
Kc(Kw)→Kw
S8
D→Kw(D)
S9
Transmitting Kw (D)
Kw(D)→D
S10
B
S11
YES
Kw updated?
S13
YES
A
Reception suspended?
To FIG. 7
NO
S14
NO
S12
YES
Kc updated?
B
NO
Reception terminated?
NO
S15
YES
Transmission terminated?
NO
YES
END

Fig. 7

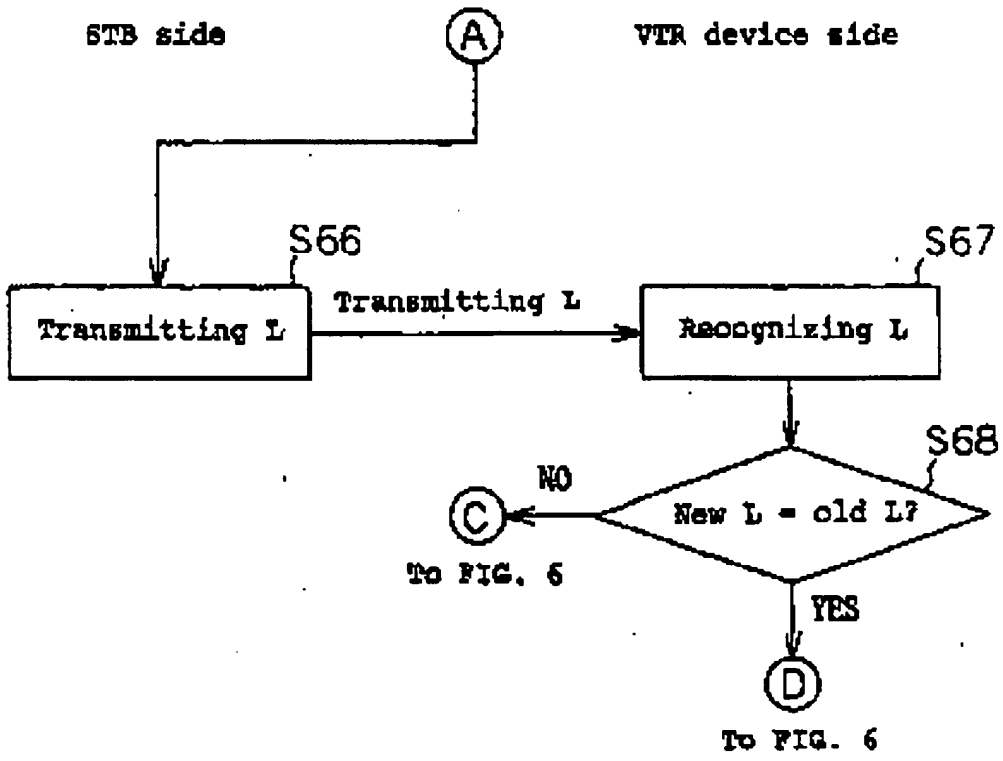

STB side
A
VTR device side
S66
Transmitting L
Transmitting L
S67
Recognizing L
S68
NO
New L = old L?
C
To FIG. 6
YES
D
To FIG. 6

Fig. 8

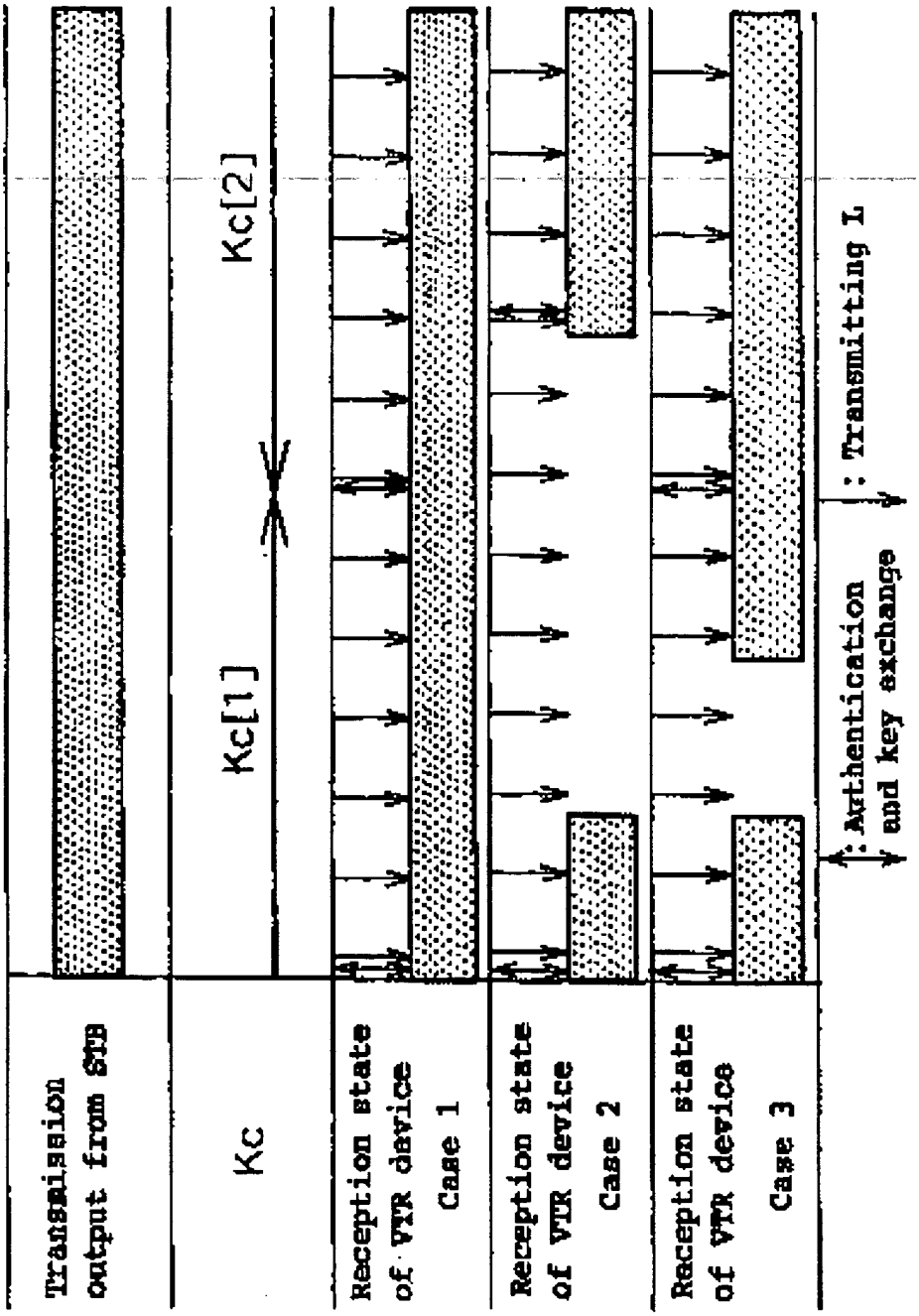

Transmission output from STB
Kc
Kc[1]
Kc[2]
Reception state of VTR device Case 1
Reception state of VTR device Case 2
Reception state of VTR device Case 3
: Authentication and key exchange
: Transmitting L

Fig. 9

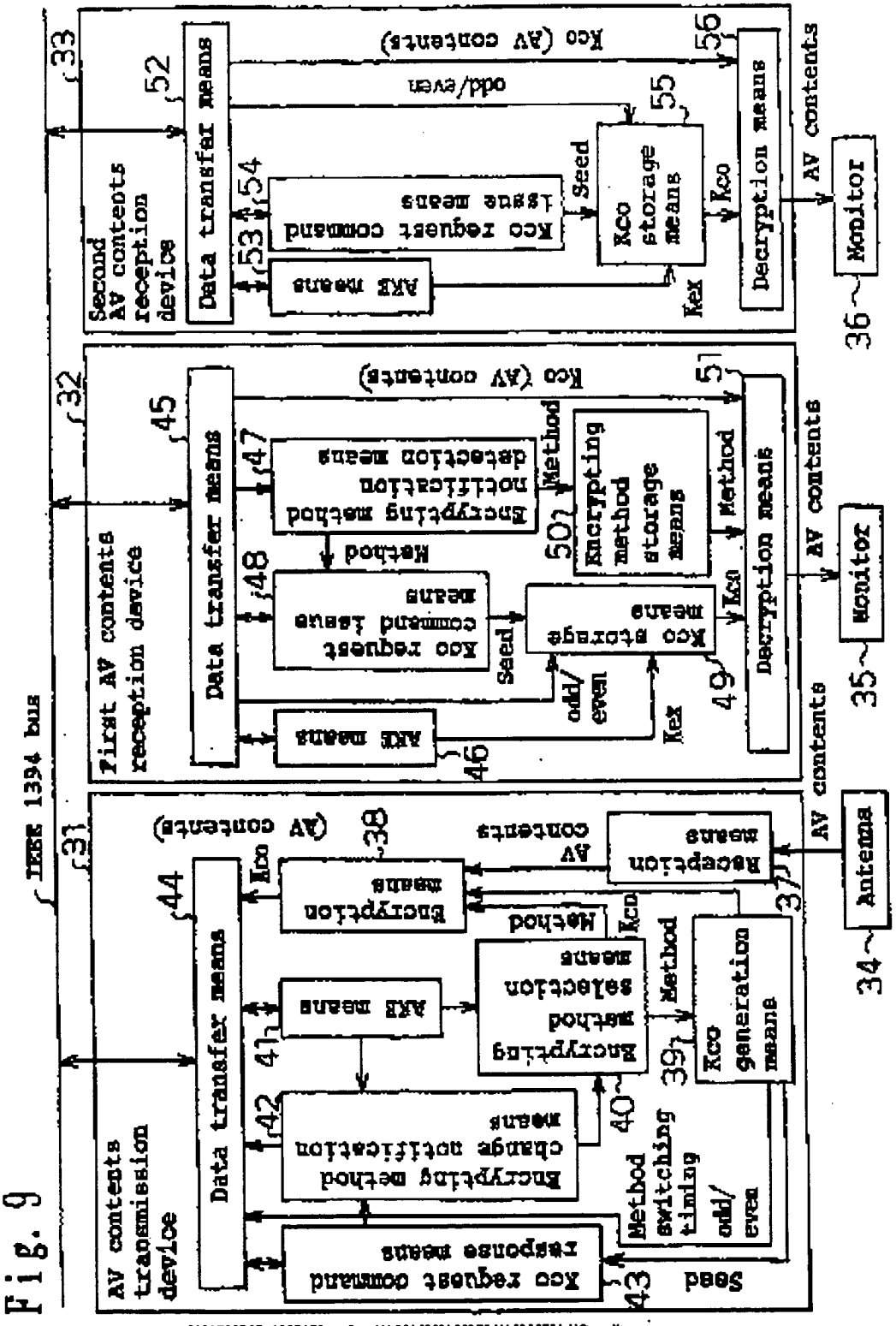

IEEE 1394 bus
AV contents transmission device
Data transfer means
Kco request command response means
Encrypting method change notification means
AKE means
Encrypting method selection means
Kco generation means
Encryption means
Reception means
Antenna
Kco (AV contents)
AV contents
Method
Method switching timing
odd/even
Seed
Kex
First AV contents reception device
Kco request command issue means
Kco storage means
Decryption means
Monitor
Second AV contents reception device
Encrypting method notification detection means
Encrypting method storage means
odd/even

Fig. 10 (a)

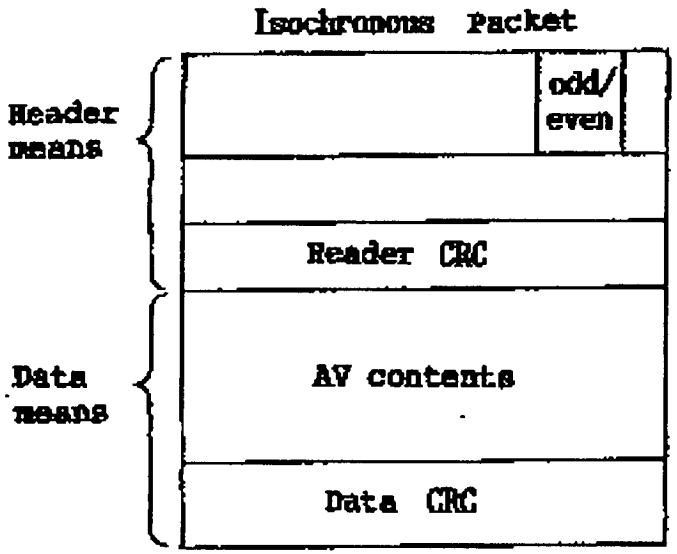
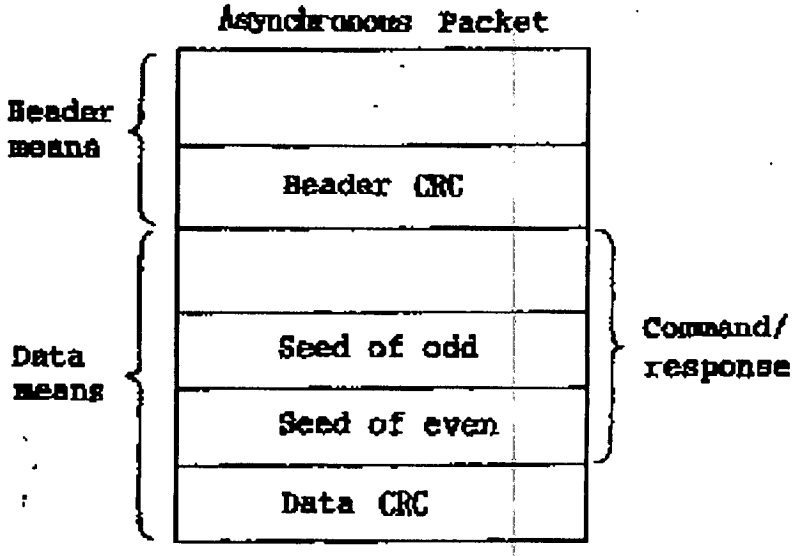


Fig. 10 (b)



EP 0 994 599 A1

Fig. 11

Operations of AV contents transmission device 31

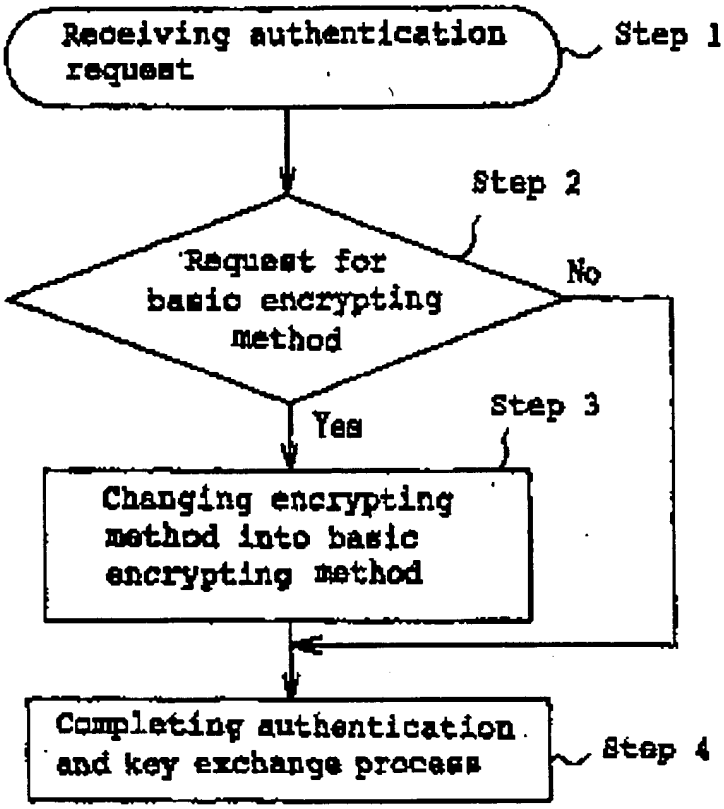


Fig. 12

Operations of first AV contents reception device 32

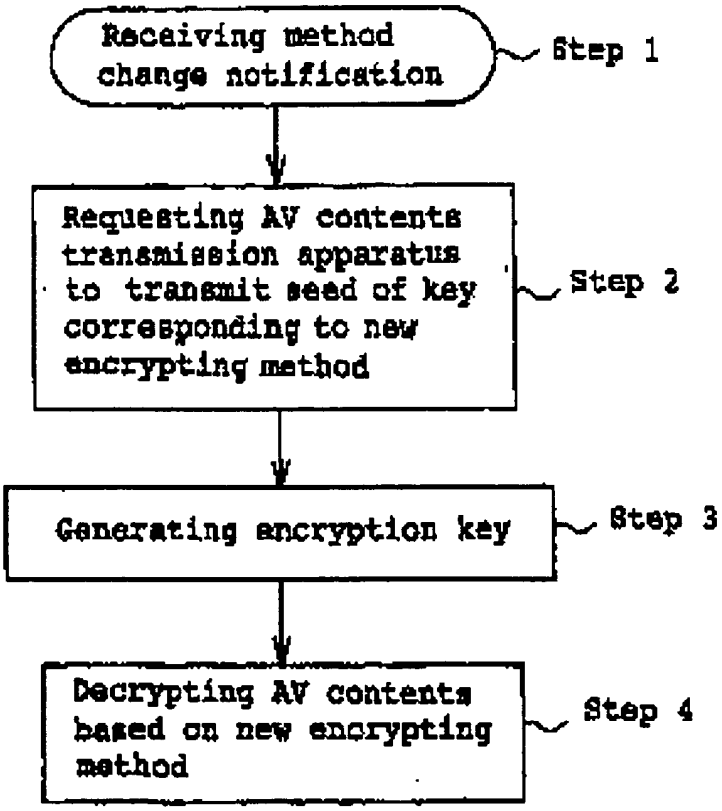


Fig. 13

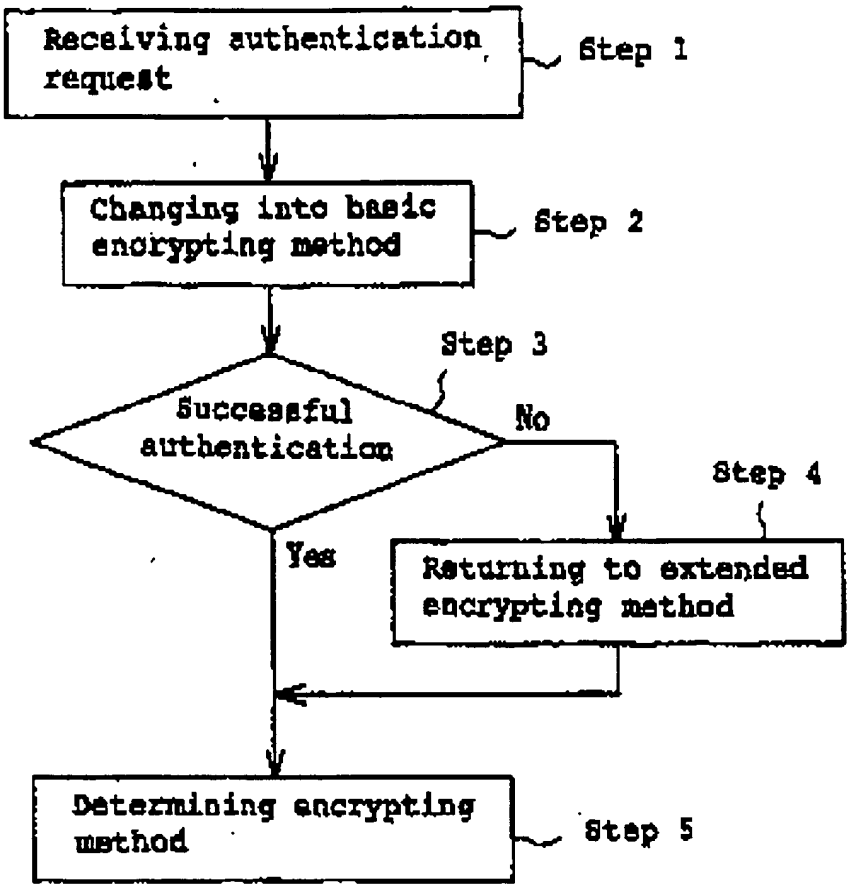

Receiving authentication request
Step 1
Changing into basic encrypting method
Step 2
Step 3
Successful authentication
No
Yes
Step 4
Returning to extended encrypting method
Determining encrypting method
Step 5

Fig. 14

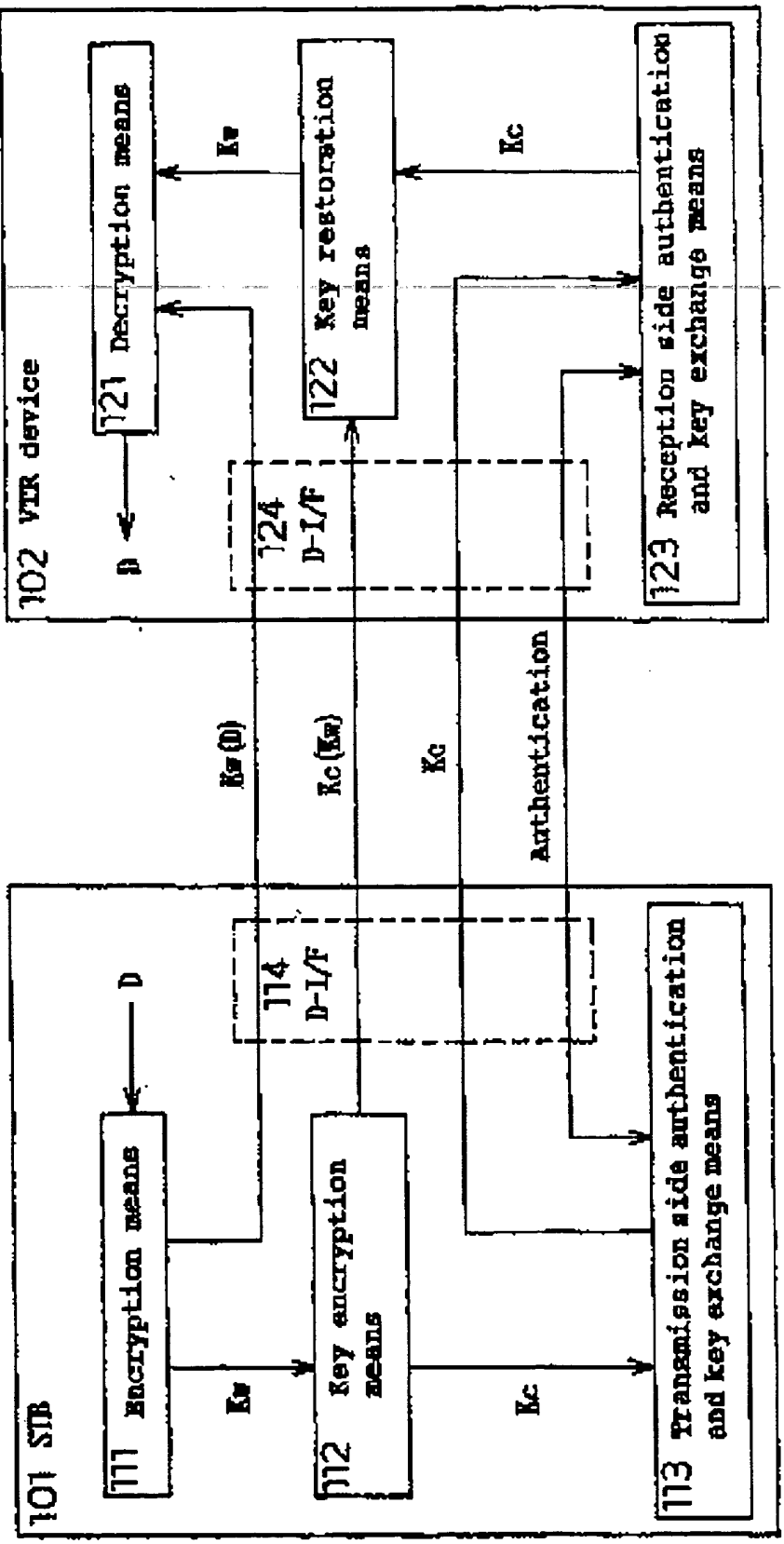
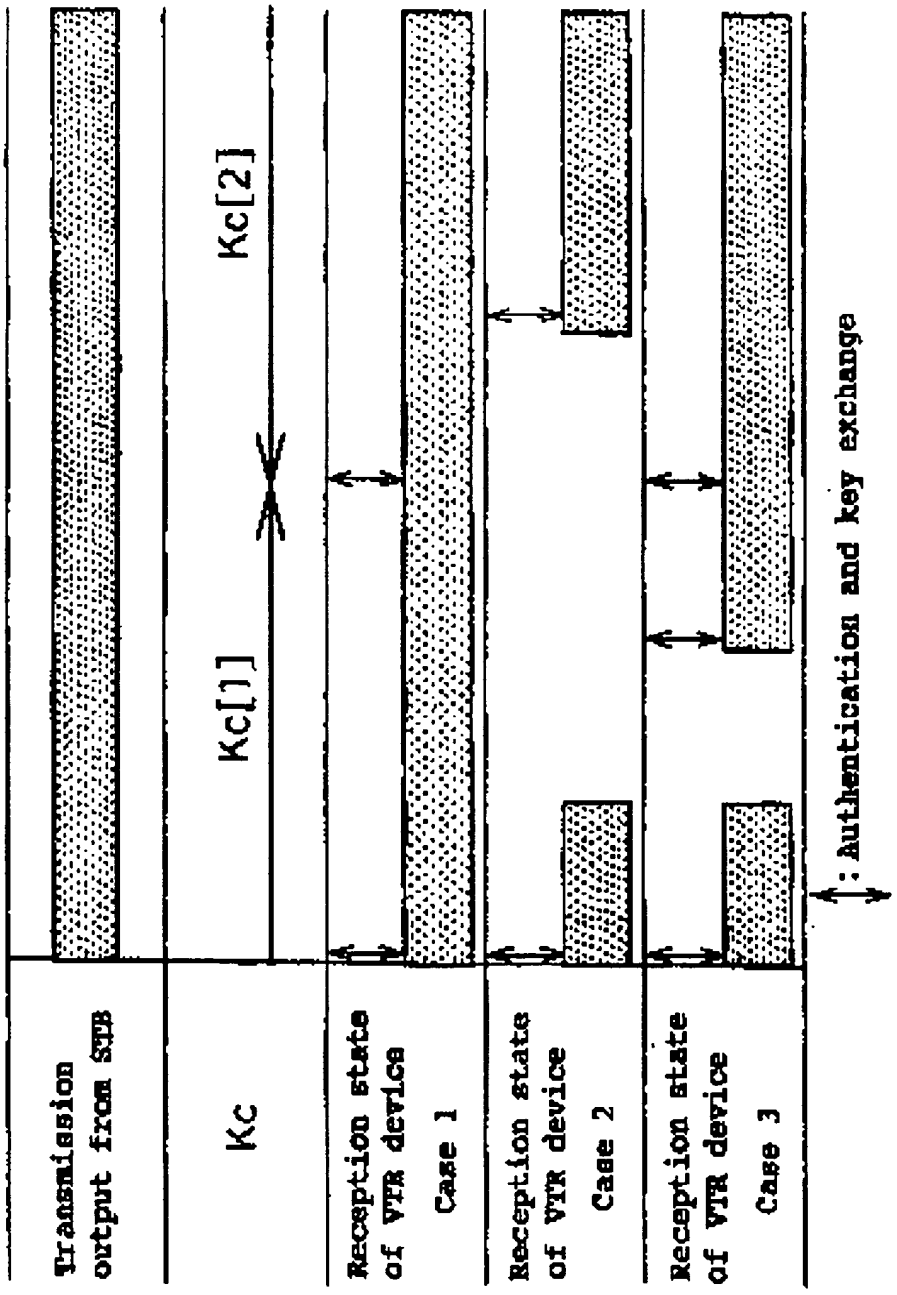

101 STB
111 Encryption means
112 Key encryption means
113 Transmission side authentication and key exchange means
114 D-I/F
D
Ks
Kc
Ks(D)
Kc(Ks)
Kc
Authentication
102 VTR device
121 Decryption means
122 Key restoration means
123 Reception side authentication and key exchange means
124 D-I/F
D
Ks
Kc

Fig. 15


Transmission output from SPB
Kc
Kc[1]
Kc[2]
Reception state of VTR device Case 1
Reception state of VTR device Case 2
Reception state of VTR device Case 3
: Authentication and key exchange

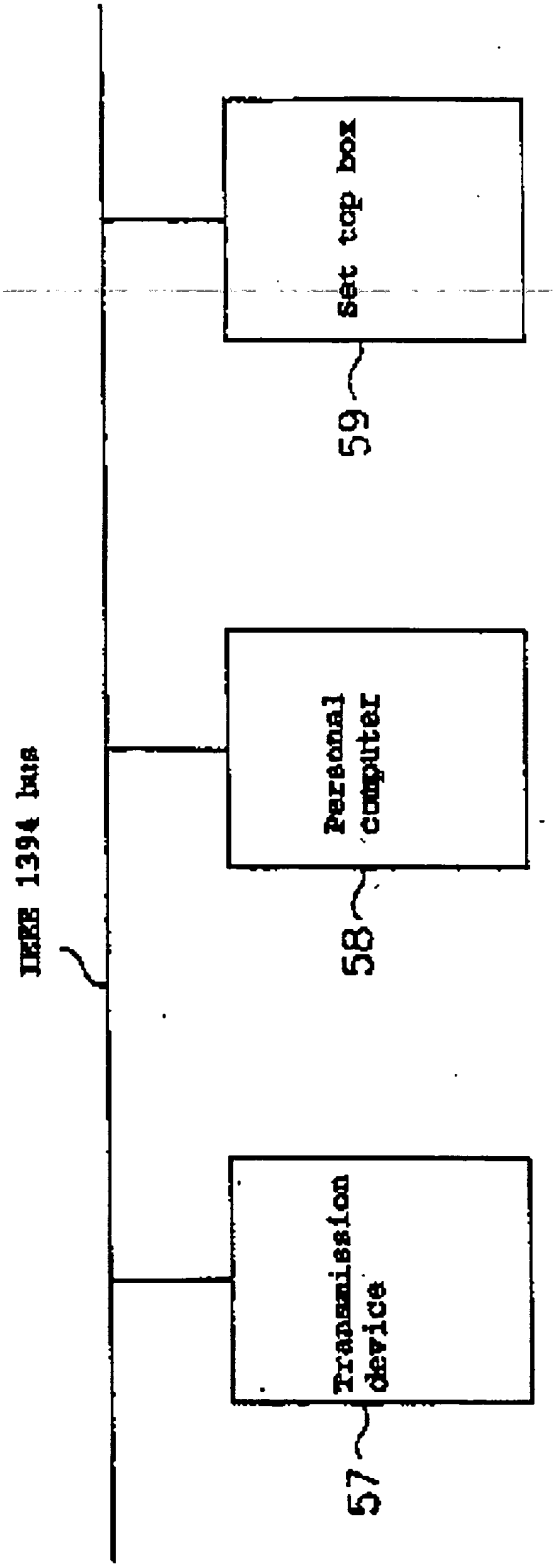

IEEE 1394 bus
Set top box
59
Personal computer
58
Transmission device
57

Fig. 16